DX Application Acceleration Platform

Command Line Reference for DXOS

Release 5.3

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 540-021499-01, Revision 1.0

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980,1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988,Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., Copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT,NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400,NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Command Line Reference for DXOS Release 5.3
Copyright © 2007, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History

22 Jun 07 —First Release

The information in this document is current as of the date listed in the revision history. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer or otherwise revise this publication without notice.

Products made or sold by Juniper Networks (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e,M160, M320, and T320 routers, T640 routing node, and the JUNOS and SDX-300 software) or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479,6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year2038. However, the NTP application is known to have some difficulty in the year 2036.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING,INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMEROR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THESOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer anon-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.

c. Other Juniper documentation for the Software (such as product purchase documents, documents accompanying the product, the Software user manual(s), Juniper's website for the Software, or messages displayed by the Software) may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, concurrent users, sessions, subscribers, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, or capabilities, or provide temporal or geographical limits.Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, or capability without first purchasing the

applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. If the Software is distributed on physical media (such as CD), Juniper warrants for 90 days from delivery that the media on which the Software is delivered will be free of defects in material and workmanship under normal use. This limited warranty extends only to the Customer. Except as may be expressly provided in separate documentation from Juniper, no other warranties apply to the Software, and the Software is otherwise provided AS IS. Customer assumes all risks arising from use of the Software. Customer's sole remedy and Juniper's entire liability under this limited warranty is that Juniper, at its option, will repair or replace the media containing the Software, or provide a refund, provided that Customer makes a proper warranty claim to Juniper, in writing, within the warranty period. Nothing in this Agreement shall give rise to any obligation to support the Software. Any such support shall be governed by a separate, written agreement. To the maximum extent permitted by law, Juniper shall not be liable for any liability for lost profits, loss of data or costs or procurement of substitute goods or services, or for any special, indirect, or consequential damages arising out of this Agreement, the Software, or any Juniper or Juniper-supplied software. In no event shall Juniper be liable for damages arising from unauthorized or improper use of any Juniper or Juniper-supplied software.

EXCEPT AS EXPRESSLY PROVIDED HEREIN OR IN SEPARATE DOCUMENTATION PROVIDED FROM JUNIPER AND TO THE EXTENT PERMITTED BYLAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE),INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR ORINTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the

license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to you may contain encryption or other capabilities restricting your ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4,FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement.

If you have any questions about this agreement, contact Juniper Networks at the following address:

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
Attn: Contracts Administrator

Table of Contents

Chapter 1 Using the Command Line Interface (CLI) 1

Accessing the CLI 1
- Using SSH to Access the CLI 2
- Using Telnet to Access the CLI 2
- Using the Console Port to Access the CLI 2

Using Online Help and Command Abbreviations 3
Applying and Saving Configuration Changes 4
Managing User Access 5
Naming Conventions 6
Typographical Conventions 6
Optional Features 7
CLI Command Summary 7

Chapter 2 Add Through Reset Config Commands 15

add Commands 15
- add activen blade 15
- add activen group 15
- add cache 16
- add cluster 16
- add ether subnet 17
- add failover peer 17
- add floatingvip 18
- add forwarder 18
- add fwlb group 18
- add gslb localdns domain 19
- add gslb remotenode 19
- add gslb resolver 19
- add gslb resolver group 20
- add gslb resolver group member 20
- add gslb resolver group servicecheck tcp port 20
- add health script 21
- add redirector 21
- add route 21
- add slb group 22
- add snat group 22
- add sync group 23
- add sync group member 23
- add user 23

arp 24
capture Commands 24
- capture file 25
- capture license 26
- capture loginbanner 26

capture ssh authorized_keys....27
capture user ssh authorized_keys....27
clear activeN Commands....27
clear activen blade stats....27
clear activen failover bindaddr....28
clear activen group advanced burst_max....28
clear activen group blade....28
clear activen group healthcheck interval....29
clear activen group healthcheck maxtries....29
clear activen group session timeout....29
clear activen group stats....30
clear activen stats....30
clear admin Commands....30
clear admin email defaultmailto....30
clear admin interface....31
clear admin log < mailto1 | mailto2 >....31
clear admin log method apprules memory level....31
clear admin log method apprules syslog facility....31
clear admin log method apprules syslog level....32
clear admin log method audit syslog facility....32
clear admin log method audit syslog level....32
clear admin log method health memory level....33
clear admin log method health syslog facility....33
clear admin log method health syslog level....33
clear admin log method system email level....33
clear admin log method system syslog facility....34
clear admin log method system syslog level....34
clear admin remoteauth ldap....34
clear admin remoteauth radius server....34
clear admin remoteauth userrole....35
clear admin scp server....35
clear admin scp username....35
clear admin snmp trap host....36
clear admin syslog facility....36
clear admin syslog host ip....36
clear admin tcpdump....37
clear admin tftp server....37
clear admin tsdump....37
clear admin webui ssl keypass....38
clear authentication cache....38
clear cache....38
clear cluster aaa authentication Commands....39
clear cluster aaa authentication ldap base-dn....39
clear cluster aaa authentication ldap gid....39
clear cluster aaa authentication ldap server....39
clear cluster aaa authentication ldap ssl cacertfile....40
clear cluster aaa authentication ldap uid....40
clear cluster aaa authentication radius server....40
clear cluster aaa authentication radius server key....41
clear cluster aaa authentication realm....41
clear cluster aaa authentication redirect host....41
clear cluster aaa authentication redirect protocol....42
clear cluster aaa authentication redirect url....42

clear cluster aaa authentication response text 42
clear cluster aaa authentication sso domain 43
clear cluster apprule ruleset 43
clear cluster apprule 43
clear cluster cache 44
clear cluster compression 44
clear cluster customiplogheader 44
clear cluster description 45
clear cluster forwardclientcert headername 45
clear cluster health request 45
clear cluster listen ssl Commands 46
clear cluster listen ssl certfile 46
clear cluster listen ssl cipherfile 46
clear cluster listen ssl clientauth cacertfile 46
clear cluster listen ssl clientauth cacrlfile 47
clear cluster listen ssl clientauth catrustfile 47
clear cluster listen ssl ephkeyfile 47
clear cluster listen ssl ephkeypass 48
clear cluster listen ssl keyfile 48
clear cluster listen ssl keypass 48
clear cluster sacompat advanced url 49
clear cluster stats 49
clear cluster sticky clientip entry 49
clear cluster target Commands 50
clear cluster target host 50
clear cluster target localip 50
clear cluster target name 50
clear cluster target ssl certfile 51
clear cluster target ssl cipherfile 51
clear cluster target ssl keyfile 51
clear cluster target ssl keypass 52
clear cluster weblog Commands 52
clear cluster weblog batch copy time 52
clear cluster weblog batch scp keyfile 52
clear cluster weblog syslog host 53
clear dns server 53
clear failover stats 53
clear forwarder Commands 54
clear forwarder description 54
clear forwarder listen ssl certfile 54
clear forwarder listen ssl cipherfile 54
clear forwarder listen ssl clientauth 55
clear forwarder listen ssl ephkeyfile 55
clear forwarder listen ssl ephkeypass 55
clear forwarder listen ssl keyfile 56
clear forwarder listen ssl keypass 56
clear forwarder stats 56
clear forwarder sticky clientip entry 57
clear forwarder target host 57
clear forwarder target localip 57
clear forwarder target ssl 58
clear fwlb Commands 58
clear fwlb group target host 58
clear fwlb group target host stats 58

clear fwlb group session 59
clear fwlb group stats 59
clear fwlb group sticky 59
clear gslb Commands 60
clear gslb agent encryption key 60
clear gslb agent stats 60
clear gslb localdns domain 60
clear gslb remotenode encryption key 61
clear gslb remotenode stats 61
clear gslb resolver group failip 61
clear gslb resolver group member stats 62
clear gslb resolver group stats 62
clear gslb resolver stats 62
clear health Commands 63
clear health remotehost host 63
clear health script 63
clear log Commands 64
clear log apprule 64
clear log audit 64
clear log health script 64
clear log system 65
clear ntp server 65
clear redirector Commands 65
clear redirector customURL 65
clear redirector description 66
clear redirector host 66
clear redirector listen ssl certfile 66
clear redirector listen ssl cipherfile 67
clear redirector listen ssl clientauth 67
clear redirector listen ssl ephkeyfile 67
clear redirector listen ssl ephkeypass 68
clear redirector listen ssl keyfile 68
clear redirector listen ssl keypass 68
clear redirector stats 69
clear server Commands 69
clear server compression 69
clear server compression cmt 69
clear server customiplogheader 70
clear server reversepath entry 70
clear server stats 70
clear slb Commands 71
clear slb failover 71
clear slb group healthcheck interval 71
clear slb group healthcheck maxtries 71
clear slb group session timeout 71
clear slb group stats 72
clear slb group sticky entry 72
clear slb group sticky timeout 72
clear slb group target host 73
clear slb group target host < ip:port | all > stats 73
clear slb stats 73
clear snat group member 74

clear sync group Commands 74
clear sync group description 74
clear sync group override filename 75
clear user role 75
clear vlan Commands 76
clear vlan all 76
clear vlan default 76
clear vlan ip 76
clear vlan range 77
clear vlan tag 77
cls 78
configure 78
copy Commands 78
copy config 79
copy file 80
copy tcpdump 81
delete Commands 81
delete activen blade 81
delete activen group 82
delete cache 82
delete cluster 82
delete config 83
delete ether subnet 83
delete failover peer 83
delete file 84
delete floatingvip 84
delete forwarder 84
delete fwlb group 85
delete gslb localdns domain 85
delete gslb remotenode 85
delete gslb resolver 86
delete gslb resolver group 86
delete gslb resolver group member 86
delete gslb resolver group servicecheck tcp port 86
delete health script 87
delete loginbanner 87
delete redirector 87
delete route 88
delete slb group 88
delete snat group 88
delete ssh authorized_keys 89
delete sync group 89
delete sync group member 89
delete tcpdump 90
delete user 90
delete user ssh authorized_keys 90
display Commands 91
display config 91
display file 91
display loginbanner 91
display users 91
exit 92

export Commands 92
export cluster stats history 93
export config 93
export log apprule 94
export log audit 94
export log health script 94
export log system 95
export ruleset 95
export snapshot system 95
export users 95
gen Commands 96
gen cac 96
gen csr 96
gen key 97
gen ssc 97
halt 97
help 98
history 98
import Commands 98
import config 99
import health certfile 99
import health script 99
import license 100
import ruleset 100
import snapshot system 100
import ssh authorized_keys 101
import user ssh authorized_keys 101
import users 101
install 102
list Commands 103
list config 103
list file 103
list tcpdump 104
netstat Commands 104
netstat N 104
netstat -a 104
netstat -s 105
netstat -r 105
ping 105
quit 106
reboot 106
reload 106
reset config 107

Chapter 3 Set Commands 109

set activen Commands 109
set activen 109
set activen advanced burst_max 109
set activen advanced policy 110
set activen advanced reset 110
set activen advanced synflood_protect 110
set activen blade < hardpaused | softpaused | unpaused > 111
set activen cleaning_interval 111
set activen failover 111

set activen group advanced burst_max....112
set activen group advanced policy....112
set activen group advanced reset....112
set activen group advanced synflood_protect....113
set activen group blade....113
set activen group blade <hardpaused | softpaused | unpaused> 113
set activen group <hardpaused | softpaused | unpaused> 114
set activen group healthcheck interval....114
set activen group healthcheck maxtries....114
set activen group session timeout....115
set activen group sticky....115
set activen group sticky failover....116
set activen healthcheck interval....116
set activen healthcheck maxtries....116
set activen max_blades....117
set activen session timeout....117
set activen sticky timeout....117
set admin Commands....118
set admin cli sessionExpireTime....118
set admin email defaultmailto....118
set admin email from....118
set admin email server....119
set admin interface ether....119
set admin log Commands....119
set admin log....120
set admin log mailto1....120
set admin log mailto2....120
set admin log method apprules memory level....121
set admin log method apprule syslog facility....121
set admin log method apprule syslog level....121
set admin log method audit showcmd....122
set admin log method audit syslog facility....122
set admin log method audit syslog level....122
set admin log method health memory level....123
set admin log method health syslog facility....123
set admin log method health syslog level....123
set admin log method system email level....124
set admin log method system memory level....124
set admin log method system syslog facility....124
set admin log method system syslog level....125
set admin remoteauth Commands....125
set admin remoteauth ldap base-dn....125
set admin remoteauth ldap bind password....125
set admin remoteauth ldap bind user-dn....126
set admin remoteauth ldap server <1 | 2> ip....126
set admin remoteauth ldap server <1 | 2> port....126
set admin remoteauth ldap uid....127
set admin remoteauth ldap version....127
set admin remoteauth protocol....127
set admin remoteauth radius server <1 | 2> ip....128
set admin remoteauth radius server <1 | 2> port....128
set admin remoteauth radius server key....128
set admin remoteauth radius server retries....129
set admin remoteauth radius server timeout....129

set admin remoteauth status 129
set admin remoteauth userrole 130
set admin scp Commands 130
set admin scp server 130
set admin scp username 131
set admin snmp Commands 131
set admin snmp community ip 131
set admin snmp community name 132
set admin snmp community netmask 132
set admin snmp contact 132
set admin snmp 133
set admin snmp location 133
set admin snmp trap 133
set admin snmp trap host < 1 | 2 > community 134
set admin snmp trap host < 1 | 2 > ip 134
set admin snmp trap host < 1 | 2 > version 134
set admin snmp trap threshold connection 135
set admin snmp trap threshold loginfail 135
set admin soap Commands 135
set admin soap < down | up > 135
set admin soap port 136
set admin soap ssl certfile 136
set admin soap ssl keyfile 136
set admin soap ssl keypass 137
set admin ssh 137
set admin stats history 137
set admin syslog Commands 138
set admin syslog facility 138
set admin syslog host < 1 | 2 > ip 138
set admin syslog host < 1 | 2 > port 139
set admin tcpdump Commands 139
set admin tcpdump capturesize 139
set admin tcpdump mailto1 < first > 139
set admin tcpdump mailto2 < second > 140
set admin telnet 140
set admin tftp server 140
set admin tsdump Commands 141
set admin tsdump filename 141
set admin tsdump mailto1 < first > 142
set admin tsdump mailto2 < second > 142
set admin tsdump transport 142
set admin upgrade Commands 143
set admin upgrade filename 143
set admin upgrade transport 143
set admin vip 144
set admin webui Commands 144
set admin webui < down | up > 144
set admin webui port 144
set admin webui sessionExpireTime 145
set admin webui ssl 145
set admin webui ssl keyfile 146
set admin webui ssl keypass 146
set boot 146

set cache Commands 147
set cache max_objects 147
set cache size 147
set clock 148
set cluster aaa audit Commands 148
set cluster aaa audit 148
set cluster aaa audit level 149
set cluster aaa authentication Commands 149
set cluster aaa authentication 149
set cluster aaa authentication cache 149
set cluster aaa authentication cache maxage 150
set cluster aaa authentication ldap anonymous 150
set cluster aaa authentication ldap base-dn 150
set cluster aaa authentication ldap bind password 151
set cluster aaa authentication ldap bind user-dn 151
set cluster aaa authentication ldap gid 151
set cluster aaa authentication ldap server <N> ip 152
set cluster aaa authentication ldap server <N> port 152
set cluster aaa authentication ldap server type 152
set cluster aaa authentication ldap ssl 153
set cluster aaa authentication ldap ssl cacertfile 153
set cluster aaa authentication ldap ssl uri 153
set cluster aaa authentication ldap uid 154
set cluster aaa authentication ldap version 154
set cluster aaa authentication method www 154
set cluster aaa authentication password empty_allowed 155
set cluster aaa authentication password maxage 155
set cluster aaa authentication password maxlength 155
set cluster aaa authentication protocol 156
set cluster aaa authentication radius server ip 156
set cluster aaa authentication radius server port 156
set cluster aaa authentication radius server key 157
set cluster aaa authentication radius server retries 157
set cluster aaa authentication radius server timeout 157
set cluster aaa authentication realm 158
set cluster aaa authentication redirect 158
set cluster aaa authentication redirect host 158
set cluster aaa authentication redirect protocol 159
set cluster aaa authentication redirect url 159
set cluster aaa authentication response text 159
set cluster aaa authentication sso cookie name 160
set cluster aaa authentication sso cookie timeout 160
set cluster aaa authentication sso 160
set cluster aaa authentication sso domain 161
set cluster apprule Commands 161
set cluster apprule 161
set cluster apprule limit retrypost 161
set cluster apprule ruleset 162
set cluster balance Commands 162
set cluster balance policy 163
set cluster balance policy urlhash <urllen> 163
set cluster cache Commands 163
set cluster cache 163
set cluster cache <disabled | enabled> 164

set cluster compression Commands 164
set cluster compression 2k_padding 164
set cluster compression browser global 164
set cluster compression browser <type> 165
set cluster compression cmt 165
set cluster compression cmt [disabled | enabled | global] 165
set cluster compression flushthreshold 166
set cluster compression force 166
set cluster compression global 166
set cluster compression http10 167
set cluster compression javascript 167
set cluster compression msoffice 167
set cluster compression octetstream 168
set cluster compression optimization 168
set cluster compression pdf 168
set cluster compression policy 169
set cluster compression sharepoint 169
set cluster compression shockwave 169
set cluster compression targetcompression encoding 170
set cluster compression targetcompression mode 170
set cluster compression <text_> 171
set cluster connbind 171
set cluster convert302protocol 171
set cluster customiplogheader 174
set cluster description 174
set cluster dsr 174
set cluster forwardclientcert headername 175
set cluster health Commands 175
set cluster health connect interval 176
set cluster health connect ssl 176
set cluster health connect timeout 176
set cluster health request <disabled | enabled> 177
set cluster health request interval 177
set cluster health request resume 177
set cluster health request returncode 178
set cluster health request size 178
set cluster health request string 178
set cluster health request timeout 179
set cluster health request urlpath 179
set cluster health request useragent 179
set cluster health retry 180
set cluster httpmethod Commands 180
Set cluster httpmethod connect 180
set cluster httpmethod extended 181
set cluster httpmethod webdav] 181
set cluster listen Commands 181
set cluster listen port 181
set cluster listen qos 182
set cluster listen ssl 182
set cluster listen ssl autochain 182
set cluster listen ssl certfile 183
set cluster listen ssl cipherfile 183
set cluster listen ssl ciphersuite all 183
set cluster listen ssl ciphersuite common 184

set cluster listen ssl ciphersuite export....184
set cluster listen ssl ciphersuite file....184
set cluster listen ssl ciphersuite strong....185
set cluster listen ssl clientauth....185
set cluster listen ssl clientauth authtype....185
set cluster listen ssl clientauth cacertfile....186
set cluster listen ssl clientauth cacrlfile....186
set cluster listen ssl clientauth catrustfile....187
set cluster listen ssl clientauth forwardclientcert....187
set cluster listen ssl clientauth forwardclientcert format....187
set cluster listen ssl....188
set cluster listen ssl ephkeyfile....188
set cluster listen ssl ephkeypass....188
set cluster listen ssl keyfile....189
set cluster listen ssl keypass....189
set cluster listen ssl protocol....189
set cluster listen targetdown....190
set cluster listen vip....190
set cluster name....190
set cluster owa....191
set cluster sacompat Commands....191
set cluster sacompat....191
set cluster sacompat advanced url....192
set cluster sacompat advanced defaults....192
set cluster stats history....192
set cluster sticky Commands....193
set cluster sticky clientip leader....193
set cluster sticky clientip timeout....193
set cluster sticky cookie expire....193
set cluster sticky cookie mask iponly....194
set cluster sticky cookie mask ipport....194
set cluster sticky cookie passheader....194
set cluster sticky failover....195
set cluster sticky method....195
set cluster target Commands....196
set cluster target host <all | ip:port>....196
set cluster target host <ip:port> <disabled | enabled>....196
set cluster target host <all | ip:port> <hardpaused | softpaused | unpaused>....196
set cluster target localip....197
set cluster target name <dns name>....197
set cluster target qos....197
set cluster target ssl....198
set cluster target ssl autochain....198
set cluster target ssl certfile....198
set cluster target ssl cipherfile....199
set cluster target ssl ciphersuite all....199
set cluster target ssl ciphersuite common....199
set cluster target ssl ciphersuite export....200
set cluster target ssl ciphersuite file....200
set cluster target ssl ciphersuite strong....200
set cluster target ssl....201
set cluster target ssl keyfile....201
set cluster target ssl keypass....201

set cluster target ssl protocol 202
set cluster target ssl timeout 202
set cluster target tune 202
set cluster transparency 205
set cluster weblog Commands 205
set cluster weblog 207
set cluster weblog batch compression 207
set cluster weblog batch copy copynow 207
set cluster weblog batch copy interval 208
set cluster weblog batch copy size 208
set cluster weblog batch copy time 208
set cluster weblog batch failure retryinterval 209
set cluster weblog batch host 209
set cluster weblog batch scp connecttest 209
set cluster weblog batch scp directory 210
set cluster weblog batch scp keyfile 210
set cluster weblog batch scp username 210
set cluster weblog delimiter 211
set cluster weblog destination 211
set cluster weblog format 211
set cluster weblog syslog host 212
set cluster weblog syslog port 212
set dns Commands 212
set dns domain 212
set dns server 213
set ether Commands 213
set ether ip 213
set ether <n> media 214
set ether mtu 214
set ether netmask 214
set failover Commands 215
set failover 215
set failover advanced 216
set failover discovery interface 216
set failover discovery port 217
set failover forcemaster 217
set failover linkfail 217
set failover listen port 218
set failover nodeid 218
set failover peer 218
set failover peer listen port 219
set failover stateful 219
set failover stateful syncinterval 219
set failover vmac ether 220
set failover vmac ether id 220
set forwarder Commands 220
set forwarder balance policy 221
set forwarder description 221
set forwarder dsr 221
set forwarder health connect interval 222
set forwarder health connect timeout 222
set forwarder health retry 222
set forwarder listen port 223
set forwarder listen qos 223

set forwarder listen ssl certfile 223
set forwarder listen ssl ciphersuite all 224
set forwarder listen ssl ciphersuite common 224
set forwarder listen ssl ciphersuite export 224
set forwarder listen ssl ciphersuite file 225
set forwarder listen ssl ciphersuite strong 225
set forwarder listen ssl clientauth 225
set forwarder listen ssl clientauth authtype 226
set forwarder listen ssl clientauth cacertfile 226
set forwarder listen ssl clientauth cacrlfile 227
set forwarder listen ssl clientauth catrustfile 227
set forwarder listen ssl 227
set forwarder listen ssl autochain 228
set forwarder listen ssl ephkeyfile 228
set forwarder listen ssl ephkeypass 228
set forwarder listen ssl keyfile 229
set forwarder listen ssl keypass 229
set forwarder listen ssl protocol 230
set forwarder listen vip 230
set forwarder name 230
set forwarder sticky clientip leader 231
set forwarder sticky clientip timeout 231
set forwarder sticky failover 231
set forwarder sticky method 232
set forwarder target host 232
set forwarder target host <ip:port> <hardpaused | softpaused | unpaused> 232
set forwarder target host <ip:port> maxconnections 233
set forwarder target host <ip:port> weight 233
set forwarder target localip 233
set forwarder target qos 234
set forwarder target ssl 234
set forwarder target ssl autochain 234
set forwarder target ssl certfile 234
set forwarder target ssl cipherfile 235
set forwarder target ssl ciphersuite all 235
set forwarder target ssl ciphersuite common 235
set forwarder target ssl ciphersuite export 236
set forwarder target ssl ciphersuite file 236
set forwarder target ssl ciphersuite strong 236
set forwarder target ssl keyfile 237
set forwarder target ssl keypass 237
set forwarder target ssl protocol 237
set forwarder target ssl timeout 238
set fwlb Commands 238
set fwlb 238
set fwlb group balance policy 238
set fwlb group healthcheck 239
set fwlb group listen 239
set fwlb group session timeout 240
set fwlb group sticky 240
set fwlb group target host 241
set fwlb group target host type 241

set gslb agent Commands 242
set gslb agent 243
set gslb agent encryption 243
set gslb agent encryption key 244
set gslb agent listen port 244
set gslb agent listen vip 244
set gslb localdns Commands 245
set gslb localdns domain a 245
set gslb localdns domain cname 245
set gslb localdns domain contact 245
set gslb localdns domain mx 246
set gslb localdns domain ns 246
set gslb localdns domain ptr 247
set gslb localdns domain sequence autoincrement 247
set gslb localdns domain sequence number 247
set gslb localdns domain ttl 248
set gslb remotenode Commands 248
set gslb remotenode agentip 248
set gslb remotenode encryption 249
set gslb remotenode encryption key 249
set gslb remotenode metricinterval 249
set gslb remotenode name 250
set gslb remotenode port 250
set gslb remotenode timeout 250
set gslb resolver Commands 251
set gslb resolver 251
set gslb resolver group dns answermode 251
set gslb resolver group dns authdomainname 252
set gslb resolver group dns authservername 252
set gslb resolver group dns hostname 252
set gslb resolver group dns ttl 253
set gslb resolver group failip 253
set gslb resolver group lba policy 254
set gslb resolver group lba sticky 254
set gslb resolver group lba sticky max 255
set gslb resolver group lba sticky netmask 255
set gslb resolver group lba sticky timeout 255
set gslb resolver group member ip 256
set gslb resolver group member remotenode 256
set gslb resolver group member weight 256
set gslb resolver group metric byterate 257
set gslb resolver group metric connections 257
set gslb resolver group metric cpuusage 258
set gslb resolver group metric defaults 258
set gslb resolver group metric memusage 258
set gslb resolver group metric rtt 259
set gslb resolver group metric rtt count 259
set gslb resolver group metric rtt netmask 259
set gslb resolver group metric rtt timeout 260
set gslb resolver group metric sessions 260
set gslb resolver group metric smoothing 260
set gslb resolver group metric targethostavailability 261
set gslb resolver group name 261
set gslb resolver group servicecheck 261

set gslb resolver group servicecheck mode 262
set gslb resolver listen port 262
set gslb resolver listen vip 262
set gslb resolver target 263
set health Commands 263
set health remotehost 263
set health remotehost host 264
set health remotehost interval 264
set health remotehost minhostsfailing 264
set health remotehost retry 265
set health remotehost startupdelay 265
set health remotehost timeout 265
set health script 266
set health script interval 266
set health script testrun 266
set health script vip 267
set hostname 267
set ntp Commands 267
set ntp 267
set ntp server 268
set password 268
set qos Commands 268
set ... qos mark outgoing 269
set ... qos mark outgoing dscp phb assured 269
set ... qos mark outgoing dscp phb class 269
set ... qos mark outgoing dscp phb class 270
set ... qos mark outgoing dscp raw 270
set ... qos mark outgoing tos ip-precedence 270
set ... qos mark outgoing tos dtrc 271
set redirector Commands 271
set redirector customurl 271
set redirector description 272
set redirector 272
set redirector dsr 272
set redirector host 273
set redirector listen port 273
set redirector listen qos 273
set redirector listen ssl certfile 273
set redirector listen ssl cipherfile 274
set redirector listen ssl ciphersuite all 274
set redirector listen ssl ciphersuite common 274
set redirector listen ssl ciphersuite export 275
set redirector listen ssl ciphersuite file 275
set redirector listen ssl ciphersuite strong 275
set redirector listen ssl clientauth authtype 276
set redirector listen ssl clientauth cacertfile 276
set redirector listen ssl clientauth cacrlfile 276
set redirector listen ssl clientauth catrustfile 277
set redirector listen ssl clientauth 277
set redirector listen ssl 277
set redirector listen ssl autochain 278
set redirector listen ssl ephkeyfile 278
set redirector listen ssl ephkeypass 278
set redirector listen ssl keyfile 279

set redirector listen ssl keypass 279
set redirector listen ssl protocol 279
set redirector listen vip 280
set redirector name 280
set redirector port 280
set redirector protocol http 281
set redirector protocol https 281
set redirector target qos 281
set redirector urlmethod custom 281
set redirector urlmethod request 282
set route default 282
set server 282
set server compression Commands 283
set server compression 2k_padding 283
set server compression browser 283
set server compression browser defaults 284
set server compression cmt 284
set server compression cmt 284
set server compression defaults 285
set server compression flushthreshold 285
set server compression force 285
set server compression http10 286
set server compression javascript 286
set server compression level 286
set server compression msoffice 287
set server compression octetstream 287
set server compression optimization 287
set server compression pdf 288
set server compression policy 288
set server compression sharepoint 288
set server compression shockwave 289
set server compression <text_> 289
set server customiplogheader 289
set server forwardclientcert headername 290
set server failover 290
set server maxconns 290
set server reversepath Commands 291
set server reversepath 291
set server reversepath maxroutes 291
set server reversepath timeout 291
set slb Commands 292
set slb 292
set slb advanced reset 292
set slb failover 292
set slb group advanced reset 293
set slb group <hardpaused | softpaused | unpaused> 293
set slb group healthcheck interval 293
set slb group healthcheck maxtries 294
set slb group healthcheck smtp 294
set slb group listen qos 294
set slb group minhosts 294
set slb group nat 295
set slb group nat port 295
set slb group policy 295

set slb group priority 296
set slb group protocol 296
set slb group service 297
set slb group session timeout 297
set slb group sticky 297
set slb group sticky failover 298
set slb group sticky leader 298
set slb group sticky softpause override 298
set slb group sticky timeout 299
set slb group target host 299
set slb group target host <hardpaused | softpaused | unpaused> 299
set slb group target host maxconns 300
set slb group target host priority 300
set slb group target host weight 301
set slb group target qos 301
set slb healthcheck interval 301
set slb healthcheck maxtries 301
set slb session timeout 302
set slb sticky timeout 302
set snat Commands 302
set snat group member 303
set snat group member ip 303
set snat group member netmask 303
set snat group vip 304
set snat idletime 304
set snat maxconn 304
set sync group Commands 305
set sync group description 305
set sync group member password 305
set sync group member port 305
set sync group member username 306
set sync group name 306
set sync group override 306
set sync group override filename 307
set sync group timeout 307
set timezone 307
set user Commands 310
set user 310
set user class 310
set user mustchange 311
set user password 311
set user role 311
set vlan Commands 312
set vlan default 312
set vlan ip 312
set vlan range 313

Chapter 4 Show Through Write Commands 315

show activen Commands 315
show activen 316
show activen advanced 316
show activen blade 316
show activen blade <ip | all> stats 316
show activen failover 317

show activen group 317
show activen group sticky entries 317
show activen group sticky failover status 318
show activen group stats 318
show activen stats 318
show activen status 318
show activen sticky timeout 319
show admin Commands 319
show admin cli 320
show admin cli sessionExpireTime 320
show admin email 320
show admin interface 321
show admin log Commands 321
show admin log mailto 321
show admin log method apprules memory level 321
show admin log method apprules syslog facility 321
show admin log method apprules syslog level 322
show admin log method audit showcmd 322
show admin log method audit syslog facility 322
show admin log method audit syslog level 323
show admin log method health memory level 323
show admin log method health syslog facility 323
show admin log method health syslog level 323
show admin log method system email level 324
show admin log method system memory level 324
show admin log method system syslog facility 324
show admin log method system syslog level 324
show admin log status 325
show admin remoteauth Commands 325
show admin remoteauth 325
show admin remoteauth ldap 325
show admin remoteauth protocol 325
show admin remoteauth radius server 326
show admin remoteauth status 326
show admin remoteauth userrole 326
show admin scp Commands 327
show admin scp 327
show admin scp server 327
show admin scp username 327
show admin snmp Commands 328
show admin snmp 328
show admin snmp community 328
show admin snmp community ip 328
show admin snmp community name 328
show admin snmp community netmask 329
show admin snmp contact 329
show admin snmp location 329
show admin snmp status 330
show admin snmp trap 330
show admin snmp trap authfailure 330
show admin snmp trap enterprise 330
show admin snmp trap generic 331
show admin snmp trap host 331
show admin snmp trap host [1 | 2] 331

show admin snmp trap host [1 | 2] community 332
show admin snmp trap host [1 | 2] ip 332
show admin snmp trap host [1 | 2] version 332
show admin snmp trap threshold 332
show admin soap Commands 333
show admin soap 333
show admin soap port 333
show admin soap ssl 333
show admin soap ssl certfile 334
show admin soap ssl keyfile 334
show admin soap ssl keypass 334
show admin soap status 335
show admin ssh 335
show admin stats history status 335
show admin syslog 335
show admin tcpdump Commands 336
show admin tcpdump 336
show admin tcpdump capturesize 336
show admin telnet 337
show admin tftp 337
show admin tsdump Commands 337
show admin tsdump 337
show admin tsdump filename 338
show admin tsdump transport 338
show admin upgrade Commands 338
show admin upgrade 338
show admin upgrade filename 339
show admin upgrade transport 339
show admin vip 339
show admin webui Commands 340
show admin webui 340
show admin webui port 340
show admin webui sessionExpireTime 340
show admin webui ssl 341
show admin webui ssl certfile 341
show admin webui ssl keyfile 341
show admin webui ssl keypass 341
show admin webui ssl status 342
show admin webui status 342
show authentication Commands 342
show authentication 342
show authentication cache 342
show authentication cache stats 343
show boot 343
show cache Commands 343
show cache 343
show cache stats 344
show cache stats < details > 344
show capacity 344
show clock 345
show cluster 345
show cluster aaa audit 345

show cluster aaa authentication Commands 346
show cluster aaa authentication 346
show cluster aaa authentication cache 346
show cluster aaa authentication cache maxage 347
show cluster aaa authentication cache status 347
show cluster aaa authentication ldap 347
show cluster aaa authentication ldap anonymous 347
show cluster aaa authentication ldap base-dn 348
show cluster aaa authentication ldap bind-dn 348
show cluster aaa authentication ldap gid 348
show cluster aaa authentication ldap server 349
show cluster aaa authentication ldap server type 349
show cluster aaa authentication ldap ssl 349
show cluster aaa authentication ldap uid 349
show cluster aaa authentication ldap version 350
show cluster aaa authentication method 350
show cluster aaa authentication password 350
show cluster aaa authentication protocol 351
show cluster aaa authentication radius server 351
show cluster aaa authentication realm 351
show cluster aaa authentication redirect 351
show cluster aaa authentication response 352
show cluster aaa authentication sso 352
show cluster aaa authentication sso cookie 352
show cluster aaa authentication sso cookie name 353
show cluster aaa authentication sso cookie timeout 353
show cluster aaa authentication sso domain 353
show cluster aaa authentication sso status 353
show cluster apprule Commands 354
show cluster apprule 354
show cluster apprule limit 354
show cluster apprule ruleset 354
show cluster apprule stats 355
show cluster apprule stats ptc 355
show cluster apprule stats pth 355
show cluster apprule stats rs 356
show cluster apprule stats rth 356
show cluster apprule status 356
show cluster balance 356
show cluster cache Commands 357
show cluster cache 357
show cluster cache stats 357
show cluster compression Commands 358
show cluster compression 358
show cluster compression 2k_padding 358
show cluster compression browser 358
show cluster compression cmt 358
show cluster compression cmt status 359
show cluster compression flushthreshold 359
show cluster compression force 359
show cluster compression http10 360
show cluster compression javascript 360
show cluster compression msoffice 360
show cluster compression octetstream 361

show cluster compression optimization 361
show cluster compression policy 361
show cluster compression shockwave 361
show cluster compression targetcompression encoding 362
show cluster compression targetcompression mode 362
show cluster compression <text_> 362
show cluster connbind 363
show cluster convert302protocol 363
show cluster customiplogheader 363
show cluster description 363
show cluster dsr 364
show cluster health Commands 364
show cluster health 364
show cluster health connect 365
show cluster health connect interval 365
show cluster health connect ssl 365
show cluster health connect timeout 365
show cluster health request interval 366
show cluster health request resume 366
show cluster health request returncode 366
show cluster health request size 367
show cluster health request status 367
show cluster health request timeout 367
show cluster health request urlpath 368
show cluster health request useragent 368
show cluster health retry 368
show cluster httpmethod 369
show cluster listen Commands 369
show cluster listen 369
show cluster listen interface 369
show cluster listen port 370
show cluster listen qos 370
show cluster listen ssl 370
show cluster listen ssl certfile 370
show cluster listen ssl cipherfile 371
show cluster listen ssl cipherlist 371
show cluster listen ssl ciphersuite 371
show cluster listen ssl clientauth 372
show cluster listen ssl clientauth authtype 372
show cluster listen ssl clientauth cacertfile 372
show cluster listen ssl clientauth cacrlfile 372
show cluster listen ssl clientauth catrustfile 373
show cluster listen ssl clientauth forwardclientcert 373
show cluster listen ssl clientauth forwardclientcert format 373
show cluster listen ssl clientauth forwardclientcert status 374
show cluster listen ssl clientauth status 374
show cluster listen ssl ephkeyfile 374
show cluster listen ssl keyfile 374
show cluster listen ssl protocol 375
show cluster listen ssl status 375
show cluster listen targetsdown 375
show cluster listen vip 376
show cluster owa 376

show cluster sacompat Commands 376
show cluster < name > sacompat [status] 376
show cluster < name > sacompat advanced 377
show cluster < name > sacompat advanced url [1 | 2 | 3] 377
show cluster stats Commands 377
show cluster stats 377
show cluster stats auth 378
show cluster stats health 378
show cluster stats history 378
show cluster stats history export 380
show cluster stats history http listen 380
show cluster stats history http listen browser 381
show cluster stats history http listen method 381
show cluster stats history http listen req-err 381
show cluster stats history http listen request 381
show cluster stats history http listen version 382
show cluster stats history http target 382
show cluster stats history http target bytesin 382
show cluster stats history http target bytesout 383
show cluster stats history http target content 383
show cluster stats history http target decompression 383
show cluster stats history http target responsecode 383
show cluster stats history io listen 384
show cluster stats history io target 384
show cluster stats history ssl 385
show cluster stats history status 385
show cluster stats http 385
show cluster stats io 386
show cluster stats ssl 386
show cluster sticky Commands 386
show cluster sticky 386
show cluster sticky clientip 386
show cluster sticky clientip entries 387
show cluster sticky cookie 387
show cluster sticky failover status 387
show cluster sticky method 388
show cluster target Commands 388
show cluster target 388
show cluster target host < ip:port > 388
show cluster target host < ip:port | all > stats 389
show cluster target host < ip:port | all > stats history 389
show cluster target host < ip:port | all > stats history http 389
show cluster target host < ip:port | all > stats history http bytesin 390
show cluster target host < ip:port | all > stats history http bytesout 390
show cluster target host < ip:port | all > stats history http content 390
show cluster target host < ip:port | all > stats history http responsecode 390
show cluster target host < ip:port | all > stats history http target decompression 391
show cluster target host < ip:port > stats history io 391
show cluster target host < ip:port | all > stats history ssl 391
show cluster target host < ip:port | all > stats http 392
show cluster target host < ip:port | all > stats io 392
show cluster target host < ip:port | all > stats ssl 392

show cluster target localip 393
show cluster target name 393
show cluster target qos 393
show cluster target ssl 394
show cluster target ssl certfile 394
show cluster target ssl cipherlist 394
show cluster target ssl ciphersuite 395
show cluster target ssl keyfile 395
show cluster target ssl protocol 395
show cluster target ssl status 395
show cluster target ssl timeout 396
show cluster target status 396
show cluster transparency 396
show cluster weblog Commands 397
show cluster weblog 397
show cluster weblog batch 397
show cluster weblog batch compression 397
show cluster weblog batch copy 397
show cluster weblog batch copy interval 398
show cluster weblog batch copy size 398
show cluster weblog batch copy time 398
show cluster weblog batch failure 399
show cluster weblog batch failure retryinterval 399
show cluster weblog batch host 399
show cluster weblog batch scp 399
show cluster weblog batch scp directory 400
show cluster weblog batch scp keyfile 400
show cluster weblog batch scp username 400
show cluster weblog delimiter 401
show cluster weblog destination 401
show cluster weblog format 401
show cluster weblog status 401
show cluster weblog syslog 402
show cluster weblog syslog host 402
show cluster weblog syslog port 402
show commands 403
show config 403
show dashboard 403
show dns Commands 404
show dns domain 404
show dns server 404
show ether 404
show failover Commands 405
show failover 405
show failover advanced 405
set failover discovery 406
show failover forcemaster 406
show failover linkfail 406
show failover listen 406
show failover nodeid 407
show failover peer 407
show failover stateful stats 407
show failover stateful status 408
show failover stateful syncinterval 408

show failover stats 408
show failover status 409
show failover vmac 409
show file 409
show flash 410
show floatingvip 410
show forwarder Commands 410
show forwarder 410
show forwarder balance 411
show forwarder balance policy 411
show forwarder description 411
show forwarder dsr 411
show forwarder health 412
show forwarder health connect 412
show forwarder health connect interval 412
show forwarder health connect timeout 413
show forwarder health retry 413
show forwarder listen 413
show forwarder stats 414
show forwarder sticky 414
show forwarder sticky clientip 414
show forwarder sticky failover status 415
show forwarder sticky method 415
show forwarder target 415
show forwarder target host 415
show forwarder target host stats 416
show forwarder target localip 416
show forwarder target qos 416
show forwarder target ssl 417
show forwarder target status 417
show fwlb Commands 417
show fwlb group 417
show fwlb status 418
show gslb Commands 418
show gslb agent 418
show gslb agent stats 418
show gslb localdns 418
show gslb localdns domain 419
show gslb remotenode 419
show gslb resolver 419
show gslb resolver group servicecheck 420
show gslb resolver group servicecheck mode 420
show gslb resolver group servicecheck status 420
show gslb resolver group servicecheck tcp port 420
show gslb resolver stats 421
show gslb resolver group stats 422
show health Commands 422
show health remotehost 422
show health script < script_name | all > interval 423
show health script < script_name | all > name 423
show health script < script_name | all > stats 423
show health script < script_name | all > status 423
show health script < script_name | all > vip 424
show hostname 424

show license Commands 424
show license 424
show license data 425
show log Commands 425
show log apprule 425
show log audit 425
show log health script 425
show log system 426
show loginbanner 426
show ntp 426
show ntpq 427
show redirector Commands 427
show redirector 427
show redirector customurl 427
show redirector description 427
show redirector dsr 428
show redirector host 428
show redirector listen 428
show redirector listen interface 429
show redirector listen port 429
show redirector listen qos 429
show redirector listen ssl 429
show redirector listen ssl certfile 430
show redirector listen ssl cipherfile 430
show redirector listen ssl cipherlist 430
show redirector listen ssl ciphersuite 431
show redirector listen ssl clientauth 431
show redirector listen ssl ephkeyfile 431
show redirector listen ssl keyfile 431
show redirector listen ssl protocol 432
show redirector listen ssl status 432
show redirector listen vip 432
show redirector port 432
show redirector protocol 433
show redirector stats 433
show redirector stats io 433
show redirector stats ssl 434
show redirector status 434
show redirector urlmethod 434
show route 434
show server 435
show server compression Commands 435
show server compression 435
show server compression 2k_padding 435
show server compression browser 436
show server compression cmt 436
show server compression cmt status 436
show server compression flushthreshold 437
show server compression force 437
show server compression http10 437
show server compression javascript 437
show server compression level 438
show server compression msoffice 438
show server compression octetstream 438

show server compression optimization 439
show server compression policy 439
show server compression shockwave 439
show server compression <text_> 439
show server customiplogheader 440
show server failover 440
show server forwardclientcert 440
show server maxconns 441
show server reversepath Commands 441
show server reversepath 441
show server reversepath entries 441
show server reversepath maxroutes 442
show server reversepath timeout 442
show server stats Commands 442
show server stats 442
show server stats auth 443
show server stats history 443
show server stats history http listen 443
show server stats history http listen browser 443
show server stats history http listen method 444
show server stats history http listen req-err 444
show server stats history http listen request 444
show server stats history http listen version 445
show server stats history http target 445
show server stats history http target bytesin 445
show server stats history http target bytesout 445
show server stats history http target content 446
show server stats history http target decompression 446
show server stats history http target responsecode 446
show server stats history io 447
show server stats history io listen 447
show server stats history io target 447
show server stats history ssl 448
show server stats history ssl listen 448
show server stats history ssl target 449
show server stats http 449
show server stats io 449
show server stats ssl 449
show server status 450
show slb Commands 450
show slb 450
show slb advanced 451
show slb failover 451
show slb group 451
show slb group advanced 451
show slb group healthcheck 452
show slb group healthcheck smtp 452
show slb group listen qos 452
show slb group minhosts 452
show slb group nat 453
show slb group nat port 453
show slb group policy 453
show slb group priority 454
show slb group protocol 454

show slb group service 454
show slb group session 454
show slb group session timeout 455
show slb group stats 455
show slb group sticky 455
show slb group sticky entries 456
show slb group sticky failover status 456
show slb group target host <ip:port> 456
show slb group target host <ip:port | all> session 457
show slb group target host <ip:port | all> stats 457
show slb group target qos 457
show slb healthcheck 457
show slb session 458
show slb session timeout 458
show slb stats 458
show slb stats errors 459
show slb stats healthcheck 459
show slb stats memory 459
show slb stats sticky 459
show slb stats ftp 460
show slb stats tftp 460
show slb status 460
show slb sticky timeout 461
show snat Commands 461
show snat 461
show snat group 461
show snat group member 462
show snat group member ip 462
show snat group member netmask 462
show snat group vip 462
show snat sessions 463
show sync group Commands 463
show sync group 463
show sync group description 463
show sync group member 464
show sync group override 464
show sync group timeout 464
show system debug 464
show system info 465
show tcpdump 465
show timezone 465
show ua 466
show user 466
show user ssh authorized_keys 467
show user ssh authorized_keys raw 467
show version 467
show vlan Commands 468
show vlan 468
show vlan default 468
show vlan ip 468
show vlan range 469
sync group 469

tcpdump Commands 469
tcpdump 470
tcpdump -i [ether < N >] 470
traceroute 470
tsdump 471
unconfigure 471
wall 472
who 472
whoami 472
write 472

Appendix A Glossary 473

Appendix B Cipher Suites 477

Appendix C Service Failover Commands 479

List of Tables

Table 1: User Roles....5
Table 2: CLI Command Summary 7
Table 3: Target Application Tune Options....203
Table 4: Target Web Server Tuning Options....203
Table 5: NTLM Authentication Tuning Options....204
Table 6: Web Log Field Definitions....206
Table 7: Time Zones....308
Table 8: activen Statistics....315
Table 9: show admin Options....319
Table 10: Browsers....378
Table 11: Methods....379
Table 12: Request Errors....379
Table 13: Request Version....379
Table 14: Content Types....380
Table 15: GSLB Resolver Statistics—Shown for TCP, UDP, and Totals....421
Table 18: SLB Switch Status....460
Table 19: Glossary....473
Table 20: SSL Ciphersuites....477

Chapter 1

Using the Command Line Interface (CLI)

The following topics describe how to use the command line interface (CLI) to configure DX devices:

- Accessing the CLI on page 1
- Using Online Help and Command Abbreviations on page 3
- Applying and Saving Configuration Changes on page 4
- Managing User Access on page 5
- Naming Conventions on page 6
- Typographical Conventions on page 6
- Optional Features on page 7
- CLI Command Summary on page 7

The DX also supports a web interface, known as the Web User Interface (WebUI). For more information about the WebUI, see the *Installation and Administration Guide for DXOS*.

Accessing the CLI

The following sections describe the different ways to access the CLI:

- Using SSH to Access the CLI on page 2
- Using Telnet to Access the CLI on page 2
- Using the Console Port to Access the CLI on page 2

Using SSH to Access the CLI

The DX can be accessed through a Secure Shell (SSH) client. SSH encrypts all traffic between you and the DX. You must have an SSH client or application installed on the client computer, and the SSH service must be enabled on the DX.

1. If you are using a command line SSH client, type the following command:

   ssh admin@<IP address of DX>

   If you are using a terminal emulator application that supports SSH, configure it to connect to the IP address of the DX. When you are prompted for the username, enter "admin" for the default account, or the name of a user account that you have created.

2. Enter the password for the DX. The % prompt indicates that you have reached the Juniper Networks DXSHELL.

3. To disconnect from DXSHELL at any time, enter the exit or quit command.

Using Telnet to Access the CLI

The DX can be accessed through a standard Telnet client. You must have a Telnet client or application installed on the client computer, and the Telnet service must be enabled on the DX.

1. If you are using a command line Telnet client, type the following command:

   telnet <IP address of DX>

   If you are using a PC with a terminal emulator application, configure the emulator to connect to the IP address of the DX.

2. You will be prompted for a username and password. Enter the username and password that you set for the DX.

3. You will see the % prompt that indicates that you have reached the Juniper Networks DXSHELL.

4. To disconnect from DXSHELL at any time, enter the exit or quit command.

Using the Console Port to Access the CLI

The DX can be accessed through a direct serial connection to the console port on the back of the unit. The console connection must be used for the first-time configuration.

1. Connect one end of the supplied null modem cable to the serial (console) port on the rear of the unit.

2. Connect the other end of the cable to the COM1 port of a PC running terminal emulation software or any standard RS-232 terminal. Use 9600 baud, 8 bits, no parity.

3. Open the terminal session and press Enter.

4. You will be prompted for a username and a password. Enter the username and password for the DX. If this is the first time that you have logged in, use the default account with the username “admin” and the password “admin”. You will see the % prompt that indicates that you have reached the Juniper Networks DXSHELL, a custom command-line interface.

5. To disconnect from DXSHELL at any time, enter the exit or quit command.

Using Online Help and Command Abbreviations

To view the online help for a command, type help before the command or type “?” after it. Type just help or “?” at the command prompt to view the list of high-level commands. Enter show commands to view a hierarchical list of all commands.

Pressing the tab key will complete a partially typed keyword, display the valid keywords with the same initial characters, or show all the options for an incomplete command.

Commands can be abbreviated, provided that you enter enough characters to identify each keyword. For example, the full command used to check health interval for cluster 1 is:

```
show cluster 1 health connect interval
```

The abbreviated command equivalent is:

```
sh clu 1 he c i
```

If a keyword is ambiguous, the possible matches are displayed:

```
cl cluster
Ambiguous keyword: “cl”
Possible matches:
clear
cls
```

User-defined names, such as cluster names, are not part of the command syntax check, and must be specified in full.

Applying and Saving Configuration Changes

When you enter a `set` or `clear` command to change the DX configuration, in most cases a "(*)" prefix is added to the command line prompt to indicate that the change does not take effect until the configuration is saved. To apply and save the configuration changes, enter the command:

```
(*) dx% write
```

If you have not entered the `write` command, you can discard your changes by reloading the active configuration:

```
(*) dx% reload
```

The following commands take effect immediately without entering a `write` command:

- Adding and removing users, setting user parameters, and setting the administrative password
- Setting the DX server up or down
- Setting a service up or down, such as SNMP, Telnet, Secure Socket Shell (SSH), or the Web User Interface (WebUI)
- Setting the Simple Object Access Protocol (SOAP) server up or down
- Enabling or disabling ActiveN, Unified Failover, or Server Load Balancer (SLB)

NOTE: Changes that take effect immediately must also be saved with a write command if you want to retain the changes after the next reboot.

In some cases, a reload command may cause the loaded configuration to be out of sync with the run-time configuration. For example, if you stop the DX server:

```
dx% set server down
DX server stopped.
(*) dx% show server status
Server: down
```

And then enter a `reload` command while the server is down:

```
(*) dx% reload
dx% show server status
Server: down    (loaded config: up)
```

The server is down, but since the currently loaded (and saved) configuration indicates that the server is enabled, rebooting the DX will restart the server.

Managing User Access

The CLI commands that a user can execute depends on the role assigned to the user's account by the administrator. In addition, the effect of various commands is also limited by the user's role. For example, users can import or export only the configuration settings that they are allowed to view or change. Table 1 describes the available user roles.

Table 1: User Roles

Role	Description and Tasks Performed
administrator	Can execute all commands on the DX. Only administrators can add new users and change user attributes.
network_administrator	Can execute all commands, except those related to SSL and user accounts.
network_operator	Can view all configuration settings, except those related to SSL, and can enable or disable the following: ■ Target servers (cannot change SLB) ■ State of services ■ Server ■ Telnet ■ Web Administration Server ■ SSH ■ SNMP
security_administrator	Can execute commands for SSL features only.
security_operator	Can view the SSL configuration and statistics, but cannot change the configuration related to those features.
user	Can view all status information and statistics, except SSL related information, and cannot make any configuration changes or service state changes to the DX.
target_operator	Same capabilities as a user, but can also pause or unpause a target host within a cluster or SLB group..

Access to the DX is controlled by a unique user name and password. Note the following:

- User names and passwords are case-sensitive.
- User names must be 4 to 16 characters; passwords must be 5 to 128 characters
- The word "all" is a reserved word and cannot be a user name.
- Users can change their own password using the `set password` command.
- Pressing the "password reset" button at the back of the DX clears the password for the default "admin" account.
- An ALERT event is sent if a user fails to log in on three consecutive attempts

Passwords and user information are not exported by the `export configuration` command. To export user information, use the `export user` command (refer to "export users" on page 95).

Naming Conventions

You can name a cluster, redirector, or forwarder at creation or after it is created. You can also rename an existing cluster, redirector, or forwarder. Note the following:

- Names are case-sensitive (up to 32 characters).
- The names “all,” “cache,” and “NULL” cannot be used as cluster names.
- Names can consist of letters and/or numbers, plus the following special characters (no spaces):

  @;$^&*() = + ! < > ,[]/_.-

- Names must be unique among clusters, redirectors, and forwarders, but the same name can be used for a cluster, redirector, and forwarder.
- If a cluster, redirector, or forwarder is created without a name, the lowest available integer is assigned as the name. For example, if you add three clusters without names, the clusters “1”, “2”, and “3” are created. If you delete cluster “2,” the other cluster names do not change. If you add another cluster without a name, the assigned name will be “2”.
- Configuration exports from previous releases contain the number of the cluster in the add command, and the remaining cluster configuration commands in the export depend on the implied numerical identifier. Using the next available integer as the implied name for a cluster mimics the behavior in previous releases. This way, imports of configurations from previous releases continue to function.

As an additional assistance for identification and purpose of clusters, redirectors, and forwarders, a “description” can be applied to individual clusters. This description is limited to 512 characters and is expected to be free-form text but may not include newlines. This allows administrators to fully describe a cluster's usage, contact information, warnings, or any other information deemed necessary.

Typographical Conventions

This following typographical conventions are used for the command syntax.

Convention	Meaning	Example
< >	Used to enclose variables for which a specific value must be substituted.	To add a named cache: `add cache <name>`
[ ]	Used to enclose command options.	To add a forwarder, the name can be omitted (a name will be assigned automatically): `add forwarder [<name>]`
|	Used to separate options where only one can be specified.	To clear one or all caches: `clear cache <name | all>`

Optional Features

Some DX features are optional, such as OverDrive, 3G Caching, and Global Server Load Balancing (GSLB). They are enabled through the use of a license key. If you wish to enable any optional features, contact your Juniper Sales Representative. For more information about licensing, see the *Installation and Administration Guide for DXOS*.

CLI Command Summary

Table 2 provides a summary of the available CLI commands.

Table 2: CLI Command Summary

Command	Description
“add activen blade” on page 15	Add an ActiveN blade.
“add activen group” on page 15	Add an ActiveN group.
“add cache” on page 16	Add a named cache.
“add cluster” on page 16	Add a new cluster.
“add ether subnet” on page 17	Add a subnet to an interface.
“add failover peer” on page 17	Add a static peer for Unified Failover.
“add floatingvip” on page 18	Add a floating virtual IP address (VIP).
“add forwarder” on page 18	Add a new forwarder.
“add fwlb group” on page 18	Add a firewall load balancer group.
“add gslb localdns domain” on page 19	Add a domain to the local DNS server.
“add gslb remotenode” on page 19	Add a remote DX node to the GSLB master.
“add gslb resolver” on page 19	Add a resolver to the GSLB master.
“add gslb resolver group” on page 20	Add a group to a resolver on the GSLB master.
“add gslb resolver group member” on page 20	Add a member to a GSLB group.
“add health script” on page 21	Add a health script.
“add redirector” on page 21	Add a redirector.
“add route” on page 21	Add a static route.
“add slb group” on page 22	Add a Server Load Balancing (SLB) group.
“add snat group” on page 22	Add a Source Network Address Translation (SNAT) group.
“add sync group” on page 23	Add a synchronization group and group members.
“add user” on page 23	Add a user name.
“arp” on page 24	Show the ARP table.
“capture Commands” on page 24	Capture displayed information and save in a file.
“clear activeN Commands” on page 27	Clear the member IP address or statistics for an ActiveN group, remove a complete ActiveN group, disassociate a blade from a group, or clear the statistics for a blade.
“clear admin Commands” on page 30	Clear administrative settings, such as TFTP, SCP, Syslog, E-Mail, interface, TSDump, TCPDump, and logging.
“clear authentication cache” on page 38	Clear the authentication cache.

Command	Description
“clear cache” on page 38	Clear statistics and cached objects for one or all 3G caches.
“clear cluster aaa authentication Commands” on page 39	Clear cluster authentication options and certificate files.
“clear cluster apprule ruleset” on page 43	Clear cluster authentication options and certification files.
“clear cluster cache” on page 44	Clear the cached objects for a cluster.
“clear cluster compression” on page 44	Clear the compression settings for a cluster to the global settings.
“clear cluster customiplogheader” on page 44	Clear the logging HTTP header for a cluster to the global setting.
“clear cluster description” on page 45	Clear a cluster description.
“clear cluster forwardclientcert headername” on page 45	Clear the client SSL certificate for a cluster to the global setting.
“clear cluster health request” on page 45	Clear the string or size requirement for a successful health check.
“clear cluster listen ssl Commands” on page 46	Clear a CA certificate file, CA CRL file, a CA trusted certificate, an ephemeral key filename, or ephemeral key password.
“clear cluster sacompat advanced url” on page 49	Clear the URLs used with the Juniper Secure Access SSL VPN (SA) solution.
“clear cluster stats” on page 49	Clear the statistics for a cluster.
“clear cluster sticky clientip entry” on page 49	Clear entries associating clients with target hosts.
“clear cluster target Commands” on page 50	Clear the target settings for a cluster.
“clear cluster weblog Commands” on page 52	Clear the Weblog settings for a cluster.
“clear dns server” on page 53	Clear one or all DNS servers.
“clear failover stats” on page 53	Clear all failover statistics.
“clear forwarder Commands” on page 54	Clear a forwarder’s description, statistics, SSL settings, target hosts, target address, or target SSL settings.
“clear fwlb Commands” on page 58	Clear the firewall load balancer settings for a group.
“clear gslb Commands” on page 60	Clear the GSLB settings for a group.
“clear health Commands” on page 63	Clear an IP address from Connectivity Failover Health Check or the statistics for a health script.
“clear log Commands” on page 64	Clear entries from the Audit, Apprule, Health, and System logs.
“clear ntp server” on page 65	Clear one or all NTP servers.
“clear redirector Commands” on page 65	Clear redirector options, or the certificate files, passwords, and keyfiles associated with a redirector’s SSL traffic.
“clear server Commands” on page 69	Clear server compression, statistics, a custom IP log header, or reverse path entries.
“clear slb Commands” on page 71	Clear Server Load Balancer (SLB) settings and statistics.
“clear snat group member” on page 74	Clear one or all members from a Source Network Address Translation (SNAT) group.
“clear sync group Commands” on page 74	Clear a synchronization group’s description or override file name.
“clear user role” on page 75	Clear one or more roles from one or all users.
“clear vlan Commands” on page 76	Clear virtual LAN settings.
“cls” on page 78	Clear the screen.
“configure” on page 78	Run the initial configuration prompts.
“copy Commands” on page 78	Copy configurations, files, and captured TCPDump information.

Command	Description
“delete Commands” on page 81	Delete clusters, forwarders, redirectors, routes, configurations, files, login banners, server load balancers, firewall load balancers, and users.
“display Commands” on page 91	Display the login banner, the contents of a file, or the CLI commands required to create the current configuration.
“exit” on page 92	End the session.
“export Commands” on page 92	Export configurations, logs, system snapshots, AppRule rulesets, and user accounts to a remote server via TFTP or SCP.
“gen Commands” on page 96	Generate an SSL private key, an SSL certificate signing request, or an SSL self-signed certificate.
“halt” on page 97	Turn off the device in preparation for disconnecting the power.
“help” on page 98	Display online help for CLI commands.
“history” on page 98	Display command history.
“import Commands” on page 98	Import a license, configurations, system snapshots, health scripts, AppRule rulesets, and user accounts via TFTP or SCP.
“install” on page 102	Download and install new firmware to a non-active partition.
“list Commands” on page 103	Display a list of files or saved configurations on the DX.
“netstat Commands” on page 104	Show network statistics.
“ping” on page 105	Verify connectivity with other network devices.
“quit” on page 106	End the session.
“reboot” on page 106	Restart the device.
“reload” on page 106	Discard all changes since the last write command.
“reset config” on page 107	Reset the configuration to the factory defaults.
“set activen Commands” on page 109	Enable or disable ActiveN or change ActiveN settings.
“set admin Commands” on page 118	Set the CLI idle timeout, default email settings, the interface used for admin traffic, and whether show commands are logged.
“set admin log Commands” on page 119	Set the logging parameters.
“set admin remoteauth Commands” on page 125	Set the remote authentication settings.
“set admin scp Commands” on page 130	Configure the SCP server and username used to import and export software upgrades, TCP dumps, and other information.
“set admin snmp Commands” on page 131	Configure support for SNMP.
“set admin soap Commands” on page 135	Configure the Simple Object Access Protocol (SOAP) server used to synchronize configurations.
“set admin ssh” on page 137	Enable or disable the SSH interface.
“set admin stats history” on page 137	Enable or disable collection of historical statistics for forwarders, clusters, and target hosts.
“set admin syslog Commands” on page 138	Configure support for one or two Syslog servers.
“set admin tcpdump Commands” on page 139	Specify where TCP dumps are sent (email address, SCP server, or TFTP server).
“set admin telnet” on page 140	Enable or disable the Telnet interface.
“set admin tftp server” on page 140	Configure the TFTP server and username used to import and export software upgrades, TCP dumps, and other information.
“set admin tsdump Commands” on page 141	Specify where technical service dumps are sent (email address, SCP server, or TFTP server).

Command	Description
“set admin upgrade Commands” on page 143	Specify the file name and SCP or TFTP server for the DX pac file used to upgrade the DX software.
“set admin vip” on page 144	Set the virtual IP address used to administer the DX.
“set admin webui Commands” on page 144	Configure the Web user interface.
“set boot” on page 146	Set the partition used for the next reboot.
“set cache Commands” on page 147	Configure a 3G cache.
“set clock” on page 148	Set the date and time manually on the DX.
“set cluster aaa audit Commands” on page 148	Configure HTTP(S) authentication auditing.
“set cluster aaa authentication Commands” on page 149	Configure HTTP(S) authentication and authorization parameters for a cluster.
“set cluster apprule Commands” on page 161	Specify an OverDrive AppRule ruleset for a cluster, and enable or disable ruleset operations.
“set cluster balance Commands” on page 162	Specify the load balancing policy for a cluster.
“set cluster cache Commands” on page 163	Specify a cache for a cluster, and enable or disable caching.
“set cluster compression Commands” on page 164	Configure compression between the DX and target web servers.
“set cluster connbind” on page 171	Enable or disable connection binding.
“set cluster convert302protocol” on page 171	Enable or disable the conversion of HTTP302 responses from HTTP to HTTPS or from HTTPS to HTTP.
“set cluster customiplogheader” on page 174	Specify a custom header for the IP log.
“set cluster description” on page 174	Specify descriptive text for a cluster.
“set cluster dsr” on page 174	Enable or disable Direct Server Return (DSR).
“set cluster forwardclientcert headername” on page 175	Set the header name of the client’s authentication certificate when client authentication is performed over SSL.
“set cluster health Commands” on page 175	Specify the content health check parameters for target servers.
“set cluster httpmethod Commands” on page 180	Enable or disable the Forward Proxy Accelerator.
“set cluster listen Commands” on page 181	Specify properties for cluster listen traffic between the DX and the client browser.
“set cluster name” on page 190	Change a cluster name.
“set cluster owa” on page 191	Enable or disable support for Outlook Web Access (OWA).
“set cluster sacompat Commands” on page 191	Enable or disable DX compatibility with the Juniper Secure Access SSL VPN (SA) solution.
“set cluster stats history” on page 192	Enable or disable the collection of cluster statistics history.
“set cluster sticky Commands” on page 193	Specify bindings between clients and target severs.
“set cluster target Commands” on page 196	Specify target host settings for a cluster.
“set cluster target tune” on page 202	Tune target host application settings for a cluster.
“set cluster transparency” on page 205	Enable or disable IP transparency.
“set cluster weblog Commands” on page 205	Configure the cluster Web log settings.
“set dns Commands” on page 212	Set the DNS domain name and DNS servers.
“set ether Commands” on page 213	Set the Ethernet IP address, media, MTU, and netmask.
“set failover Commands” on page 215	Configure Unified Failover.
“set forwarder Commands” on page 220	Configure forwarding of non-HTTP TCP traffic.

Command	Description
“set fwlb Commands” on page 238	Configure firewall load balancing.
“set gslb agent Commands” on page 242	Configure the agent for Global Server Load Balancing (GSLB).
“set gslb localdns Commands” on page 245	Configure the internal DNS server on the GSLB master.
“set gslb remotenode Commands” on page 248	Identify each remote node on the GSLB master.
“set gslb resolver Commands” on page 251	Configure a resolver on the GSLB master.
“set health Commands” on page 263	Configure scriptable health checking.
“set hostname” on page 267	Set the host name of the DX device.
“set ntp Commands” on page 267	Enable or disable NTP support and identify up to three NTP servers.
“set password” on page 268	Allows users to change their own password.
“set qos Commands” on page 268	Configure QoS ToS/DSCP settings for client and server traffic.
“set redirector Commands” on page 271	Configure redirection properties.
“set route default” on page 282	Set the default route.
“set server” on page 282	Enable or disable the DX server.
“set server compression Commands” on page 283	Configure DX server compression.
“set server customiplogheader” on page 289	Specify the custom header name added to client requests.
“set server forwardclientcert headername” on page 290	Specify the custom HTTP header used for SSL client certificate forwarding.
“set server maxconns” on page 290	Specify the maximum number of simultaneous server connections.
“set server reversepath Commands” on page 291	Configure DX server reverse path feature.
“set slb Commands” on page 292	Configure the Server Load Balancing (SLB) properties.
“set snat Commands” on page 302	Configure a Source Network Address Translation (SNAT) group or to add members to a group.
“set sync group Commands” on page 305	Specify a group of DX devices for configuration synchronization.
“set timezone” on page 307	Specify the DX time zone.
“set user Commands” on page 310	Manage user accounts, roles, and passwords.
“set vlan Commands” on page 312	Specify VLAN parameters.
“show activen Commands” on page 315	Show the ActiveN configuration.
“show admin Commands” on page 319	Show the CLI idle timeout, default email settings, the interface used for admin traffic, and whether show commands are logged.
“show admin remoteauth Commands” on page 325	Show the administrator remote authentication settings.
“show admin scp Commands” on page 327	Show the SCP server and username used to import and export software upgrades, TCP dumps, and other information.
“show admin snmp Commands” on page 328	Show the SNMP configuration.
“show admin soap Commands” on page 333	Show the Simple Object Access Protocol (SOAP) server used to synchronize configurations.
“show admin ssh” on page 335	Show the status of the SSH interface.
“show admin stats history status” on page 335	Show whether collection of historical statistics for forwarders, clusters, and target hosts services is enabled.
“show admin syslog” on page 335	Show the Syslog configuration.

Command	Description
“show admin tcpdump Commands” on page 336	Shows where TCP dumps are sent (email address, SCP server, or TFTP server).
“show admin telnet” on page 337	Show the status of the Telnet interface.
“show admin tftp” on page 337	Shows the TFTP server and username used to import and export software upgrades, TCP dumps, and other information.
“show admin tsdump Commands” on page 337	Shows where technical service dumps are sent (email address, SCP server, or TFTP server).
“show admin upgrade Commands” on page 338	Show the file name and SCP or TFTP server for the DX pac file used to upgrade the DX software.
“show admin vip” on page 339	Show the virtual IP address used to administer the DX.
“show admin webui Commands” on page 340	Show the Web user interface configuration.
“show authentication Commands” on page 342	Show the configuration and statistics for the authentication cache.
“show boot” on page 343	Show the status of the boot partitions.
“show cache Commands” on page 343	Show the configuration and statistics for a 3G cache.
“show capacity” on page 344	Show CPU and memory usage, and the amount of network and interface traffic in and out of the DX.
“show clock” on page 345	Show DX date and time.
“show cluster” on page 345	Show the configuration for one or all clusters.
“show cluster aaa audit” on page 345	Show whether HTTP(S) authentication auditing is enabled.
“show cluster aaa authentication Commands” on page 346	Show the HTTP(S) authentication and authorization settings for a cluster.
“show cluster apprule Commands” on page 354	Show an OverDrive AppRule ruleset for a cluster.
“show cluster balance” on page 356	Show the load balancing policy for a cluster.
“show cluster cache Commands” on page 357	Show the caches for a cluster or the cache statistics.
“show cluster compression Commands” on page 358	Show compression settings between the DX and target web servers.
“show cluster connbind” on page 363	Show whether connection binding is enabled for a cluster.
“show cluster convert302protocol” on page 363	Show whether HTTP302 responses are converted from HTTP to HTTPS or from HTTPS to HTTP.
“show cluster description” on page 363	Show the descriptive text for a cluster.
“show cluster dsr” on page 364	Show whether Direct Server Return (DSR) is enabled.
“show cluster health Commands” on page 364	Show the content health check settings for target servers.
“show cluster httpmethod” on page 369	Show the HTTP methods enabled for the Forward Proxy Accelerator.
“show cluster listen Commands” on page 369	Show the settings for cluster listen traffic between the DX and the client browser.
“show cluster owa” on page 376	Show whether support for Outlook Web Access (OWA) is enabled.
“show cluster sacompat Commands” on page 376	Show Juniper Secure Access SSL VPN (SA) solution compatibility for one or more clusters.
“show cluster stats Commands” on page 377	Show statistics for one or all clusters.
“show cluster sticky Commands” on page 386	Show bindings between clients and target severs.
“show cluster target Commands” on page 388	Show the target host settings for a cluster.
“show cluster transparency” on page 396	Show whether client IP transparency is enabled.
“show cluster weblog Commands” on page 397	Show the cluster Web log settings.

Command	Description
“show commands” on page 403	Show a hierarchical list of all CLI commands.
“show config” on page 403	Show all configuration settings.
“show dashboard” on page 403	Show a summary of the DX health and performance.
“show dns Commands” on page 404	Show the DNS server addresses and the name service domain.
“show ether” on page 404	Show the Ethernet addresses, subnets, media, MTU, and netmask.
“show failover Commands” on page 405	Show the Unified Failover configuration and statistics.
“show file” on page 409	Show the contents of a file.
“show flash” on page 410	Show the total, used, and available Flash disk space on the active partition.
“show floatingvip” on page 410	Show the floating VIP addresses.
“show forwarder Commands” on page 410	Show the configuration and statistics for forwarding non-HTTP TCP traffic.
“show fwlb Commands” on page 417	Show the configuration and statistics for the firewall load balancer.
“show gslb Commands” on page 418	Show the Global Server Load Balancing (GSLB) configuration.
“show health Commands” on page 422	Show the configuration and statistics for health checking.
“show hostname” on page 424	Show the DX host name.
“show license Commands” on page 424	Show the current licensed features and license key data.
“show log Commands” on page 425	Show the audit, AppRule, health, and system logs.
“show loginbanner” on page 426	Show the login banner.
“show ntp” on page 426	Show the NTP configuration.
“show ntpq” on page 427	Show the results of an NTP server query.
“show redirector Commands” on page 427	Show the configuration and statistics for a redirector.
“show route” on page 434	Show the default route for the DX.
“show server” on page 435	Show the configuration for the DX server.
“show server compression Commands” on page 435	Show the server compression settings.
“show server customiplogheader” on page 440	Show the custom header name added to client requests.
“show server forwardclientcert” on page 440	Show the SSL client certificate HTTP header.
“show server maxconns” on page 441	Show the maximum number simultaneous of server connections.
“show server reversepath Commands” on page 441	Show the configuration for reverse path routing.
“show server stats Commands” on page 442	Show the server statistics.
“show slb Commands” on page 450	Show the configuration and statistics for Server Load Balancing (SLB).
“show snat Commands” on page 461	Show the Source Network Address Translation (SNAT) configuration.
“show sync group Commands” on page 463	Show the synchronization configuration for a DX group.
“show system debug” on page 464	Show system debug information.
“show system info” on page 465	Show the DX hardware model and current software version.
“show tcpdump” on page 465	Show the collected TCP dump information.
“show timezone” on page 465	Show the current time zone on the DX or a list of all time zones.
“traceroute” on page 470	Show the route of packets sent to a specified destination.
“show ua” on page 466	Show the End User License Agreement.
“show user” on page 466	Show the role and status of one or all users.

Command	Description
“show version” on page 467	Show the software version on the active partition.
“show vlan Commands” on page 468	Show the collected VLAN settings.
“sync group” on page 469	Synchronize the configuration settings across a group of DXs.
“tcpdump Commands” on page 469	Captures a dump of the TCP traffic going through the DX.
“traceroute” on page 470	Shows the route of packets sent to a specific host name or IP address.
“tsdump” on page 471	Send a technical service dump to an SCP or TFTP server or to a configured E-mail address.
“unconfigure” on page 471	Restores the DX to the its original manufacturing configuration.
“wall” on page 472	Send a message to all logged in users.
“who” on page 472	Display the users who are currently logged in.
“whoami” on page 472	Display the current user name.
“write” on page 472	Save the configuration.

Chapter 2

Add Through Reset Config Commands

This chapter describes the add through reset config CLI commands.

add Commands

Use the add command to create a new ActiveN blade, group, cluster, forwarder, redirector, user, server load balancer, or a route.

add activen blade

Description Adds a new ActiveN blade. An index is returned. For additional information, see the "ActiveN" chapter of the *Installation and Administration Guide for DXOS*. This command requires an ActiveN license before it can be used.

This command does not take effect until after a `write` operation.

Syntax

```
add activen blade <real ip>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

add activen group

Description Adds a new ActiveN group with optional name and VIP and port. For additional information, see the "ActiveN" chapter of the *Installation and Administration Guide* for DXOS. This command requires an ActiveN license before it can be used.

This command does not take effect until after a `write` operation.

Syntax

```
add activen group [name] <ip:port>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

add cache

Description Adds a named cache. The name can be up to 32 characters long and can be any valid character string and may be integer-only.

Reserved DXSHELL keywords such as “all”, “none”, and “?” are considered invalid.

This command does not take effect until after a `write` operation.

Syntax `add cache <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

Examples `add cache secureImages-01_01`
Adds a 3G Cache named secureImages-01_01.

```
dx% add cache secureImages-01_01
Cache secureImages-01_01 added
(*) dx2%
```

add cluster

Description Adds a new cluster. For additional information on naming conventions, see “Naming Conventions” on page 6.

This command does not take effect until after a `write` operation.

Syntax `add cluster <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Examples

`add cluster marketing`

Add a new cluster with the name “marketing”. The response will be:

```
dx% add cluster marketing
Created cluster marketing
(*) dx2% add cluster marketing
Error: duplicate name marketing
```

You can then set the attributes of the cluster.

`add cluster`
Add a new cluster without a specified name; a default name will be assigned. The response will be:

```
dx% add cluster
Created cluster <default name>
(*) dx2%
```

You can then set the attributes of the cluster.

add ether subnet

Description Adds a subnet to an interface.

This command does not take effect until after a `write` operation.

Syntax `add ether <id> subnet <ip> <netmask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

add failover peer

Description Adds a static DX peer for Unified Failover.

This command does not take effect until after a `write` operation.

Syntax `add failover peer <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

add floatingvip

Description Adds a floating VIP. This command requires an ActiveN license before it can be used.

This command does not take effect until after a `write` operation.

Syntax `add floatingvip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

add forwarder

Description Adds a new forwarder.

This command does not take effect until after a `write` operation.

Syntax `add forwarder <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Example `add forwarder`
Add a new forwarder without a specified name. The response will be:

```
dx% add forwarder
Created forwarder <default name>
(*) dx2%
```

You can then set the attributes of the forwarder.

add fwlb group

Description Adds a new firewall load-balancing group.

The firewall balancer group name is an alphanumeric value (maximum of 32 characters). The name may be a virtual IP address and port combination (vip:port format), or a network virtual IP address and port combination (networkvip:port format). Wildcards may be used. If no value is entered, a default name is assigned.

This command does not take effect until after a `write` operation.

Syntax `add fwlb group <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

add gslb localdns domain

Description Adds a domain to the DNS Server. This adds a start of authority record for the specified domain.

This command does not take effect until after a `write` operation.

Syntax `add gslb localdns domain <domain>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add gslb remotenode

Description Adds a remote node on the GSLB master. If you omit the name, a name is generated automatically. The keywords “all" and "internal" are reserved. The maximum number of remote GSLB nodes is determined by the DX license. The name can be changed with a `set` command.

This command does not take effect until after a `write` operation.

Syntax `add gslb remotenode <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add gslb resolver

Description Adds a resolver on the GSLB master. If you omit the name, a name is generated automatically. The name can be changed with a `set` command.

This command does not take effect until after a `write` operation.

Syntax `add gslb resolver <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add gslb resolver group

Description Adds a GSLB group to a resolver. If you omit the group name, a name is generated automatically. The group name can be changed with a `set` command.

This command does not take effect until after a `write` operation.

Syntax `add gslb resolver <name> group <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add gslb resolver group member

Description Adds a member to a GSLB group. Each member represents a DX node to be load balanced. If you omit the member name, a name is generated automatically. The maximum number of members per group is determined by the DX License.

This command does not take effect until after a `write` operation.

Syntax `add gslb resolver <name> group <name> member <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add gslb resolver group servicecheck tcp port

Description Determines the ports included in the TCP service check. Port range is from 1 to 65535. Service checking mode must be set to TCP for ports to be checked.

Syntax `add gslb resolver <name> group <name> servicecheck tcp port <port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

add health script

Description Adds a new health script.

This command does not take effect until after a `write` operation.

Syntax `add health script <script_name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Health Checking

add redirector

Description Adds a new redirector.

This command does not take effect until after a `write` operation.

Syntax `add redirector <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

add route

Description Adds a static route. The default is set to 255.255.255.255 which represents a host route.

This command does not take effect until after a `write` operation.

Syntax `add route <destination> <gateway> [netmask]`

- `destination`: The IP address of the destination network.
- `gateway`: The IP address of the router you want to use.
- `netmask`: An optional parameter. It is used to set the netmask for the route that you want to use.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

add slb group

Description Adds a new Server Load Balancer (SLB) group with optional name, VIP, and port.

This command does not take effect until after a `write` operation.

Syntax `add slb group <name> <ip:port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

add snat group

Description Adds a new Source Network Address Translation (SNAT) group. The name is optional. If a name is not provided, a name starting from "1" will be allocated.

This command does not take effect until after a `write` operation.

Syntax `add snat group [name]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

add sync group

Description Creates a synchronization group. Starting with software release 4.1.15, the `add sync group` command is disabled on the DX 3670 Application Acceleration Platform.

This command does not take effect until after a `write` operation.

Syntax `add sync group <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

add sync group member

Description Adds a member to the synchronization group. `<memberid>` is either a `<hostname>` or an `<ip>`. Starting with software release 4.1.15, the `add sync group` command is disabled on the DX 3670 Application Acceleration Platform.

This command does not take effect until after a `write` operation.

Syntax `add sync group <name> member <memberid>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

add user

Description Use the `add user` command to add a new user for managing the DX. After adding the new user, you must assign a role, set the password, and enable the user account. A default user role is “none” and can access only the following commands:

```
%cls                    %exit
%help                   %history
%quit                   %set password
%show cluster           %show commands
%show forwarder         %show hostname
%show redirector        %show servers
%show support           %show ua
%show version           %who
%whoami
```

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `add user [name]`

Adds a new user for managing the DX with the <username> specified. If a username is not supplied, you will be prompted to enter one. The username must be between four and sixteen characters long.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

arp

Description Shows the ARP table.

Syntax `arp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

capture Commands

Use the `capture` command to capture data entered on the screen into a file on the DX. This command is used to capture login banners, SSL keys or certificates, or license information from the terminal into the DX.

This operation is used for capturing login banners, SSL keys, SSL Certificates, and the license key for the DX into a file. To capture the file, you paste the contents of the file “into the console” and then end the file with a period on a blank line.

The login banner allows for some print-style substitutions, as follows:

```
%h hostname
%d date
%s system (“Juniper Networks”)
%v product version
%b product build id
%% show the percent character
```

When the banner display encounters one of these substitution strings, it extracts the information from the appropriate place in the operating system and displays it. This information cannot be changed by the user.

Note that you can put HTML in your login banner, and it will display correctly on the WebUI. However, the DX does not parse out HTML code when displaying the banner on the Command Line Interface (CLI), so the HTML code will be displayed along with the desired banner.

This command does not take effect until after a `write` operation.

capture file

Description Captures displayed information and saves it to a file on the DX. This is typically used for capturing SSL keys and certificates, but can be used to create any kind of file.

Syntax

```
capture file <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

Example

```
capture file my_key
```

Start by capturing an SSL Key from the terminal and name it “my_key”. You will need to paste the content of the file and end the file with a period on a blank line. An example of the output is:

```
dx% capture file my_key
Enter file. End with period on a blank line.
-----BEGIN CERTIFICATE-----
MIIDejCCAuOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBizELMAkGA
EjAQBgNVBAgTCURFTU8gT05MWTESMBAGA1UEBxMJREVNTyBPT
EwlERU1PIE9OTFkxEjAQBgNVBAsTCURFTU8gT05MWTESMBAGA1
TkxZMRgwFgYJKoZIhvcNAQkBFglERU1PIE9OTFkwHhcNMDIwMzA1
MDIwMzA2MjM1MzAxWjCBizELMAkGA1UEBhMCWFgxEjAQBgNVBA
WTESMBAGA1UEBxMJREVNTyBPTkxZMRIwEAYDVQQKEwlERU1P
BAsTCURFTU8gT05MWTESMBAGA1UEAxMJREVNTyBPTkxZMRgw
FglERU1PIE9OTFkwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoG
HkubHFrpC1tub2CEANVBJsXfk/n8rIe/JlXCm2Gv1Q85Fk6pWh8P597r
gQE/1xBaSEwJv4GuVPtfcGyG8PJmAkoO0d/OkYsYHlZJG7aIMmJB1
mFIgT9EJ7nZAyE/Rb1p6dmJBNZYtOMaXAgMBAAGjgeswgegwHQY
MnFJOsgvF3B4HuaX9fBBDk9xMIG4BgNVHSMEgbAwga2AFCCeMn
9fBBDk9xoYGRpIGOMIGLMQswCQYDVQQGEwJYWDESMBAGA1U
MRIwEAYDVQQHEwlERU1PIE9OTFkxEjAQBgNVBAoTCURFTU8gT
CxMJREVNTyBPTkxZMRIwEAYDVQQDEwlERU1PIE9OTFkxGDAW
CURFTU8gT05MWYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb
L8dbydfkNbydH3wHcF5uUuLG5rajGzput7GrQEjKUmKEB+bI/VIRbPQ
W0FOiR7MsY64y5cbpMoGrfZ2qNgNKF+i6WLlmTfh4+1tKiCMnhTRP
hivbsYqWBdOFwrkqAUapuUDwctaAxV2pwJos47IO
-----END CERTIFICATE-----
.

dx% list file
democert
demokey
my_key
```

capture license

Description Captures the license key for the DX. The source can be the console, Telnet, or SSH.

This command does not take effect until after a `write` operation.

Syntax

```
capture license
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

Example

```
capture license
```

Installs the license key for the appliance by capturing the license key text. The key text can be typed in or pasted from the console, telnet, or SSH.

capture loginbanner

Description Captures a custom login banner. The maximum size that can be captured is 2000 characters, including newline characters.

This command does not take effect until after a `write` operation.

Syntax

```
capture loginbanner
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

Examples

```
capture loginbanner
“Unauthorized access to or use of this system is prohibited.
All access and use may be monitored and recorded.”
.

Sets the login banner to:
“Unauthorized access to or use of this system is prohibited.
All access and use may be monitored and recorded.”
```

```
dx% capture loginbanner
Enter banner. End with . on a blank line.

%%h hostname: %h
%%d date: %d
%%s system: %s
%%v version: %v
%%b build id: %b
.
Banner saved.
```

```
dx% show loginbanner

%h hostname: dx5.juniper.net
%d date: Tue Mar 24 19:18:32 PDT 2006
%s system: Juniper Networks
%v version: 5.1.0
%b build id: 0
```

Sets the login banner to show critical parameters.

capture ssh authorized_keys

Description Captures the user's public SSH key to a file on the DX and names the file authorized_keys.

Syntax `capture ssh authorized_keys`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

capture user ssh authorized_keys

Description Captures the specified user's public SSH key and saves the file to the DX. The file name is authorized_keys.

Syntax `capture user [name] ssh authorized_keys`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear activeN Commands

Use the `clear activen` commands to clear ActiveN server settings. This includes resetting the member IP Address or statistics for a group, and removing a complete ActiveN group. This command can also be used to disassociate a blade from a group, or to clear the statistics for a blade. These commands require an ActiveN license before they can be used.

clear activen blade stats

Description Clears the statistics for a blade.

This command does not take effect until after a `write` operation.

Syntax `clear activen blade <ip> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen failover bindaddr

Description The service-specific failover commands are listed in “Service Failover Commands” on page 479. These commands have been replaced by the commands for Unified Failover (refer to “set failover Commands” on page 215). .

clear activen group advanced burst_max

Description Clears the maximum number of timed out sessions that are purged in one timer interval for one or all ActiveN groups, which causes all timed-out sessions to be purged in each timer cycle.

This command does not take effect until after a `write` operation.

Syntax `clear activen group <name | all> advanced burst_max`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen group blade

Description Disassociates one or all blades from one or all ActiveN groups.

This command does not take effect until after a `write` operation.

Syntax `clear activen group <name | all> blade <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen group healthcheck interval

Description Resets the healthcheck interval settings to the default values for one or all ActiveN groups.

This command does not take effect until after a `write` operation.

Syntax `clear activen group <name | all> healthcheck interval <down | syn |up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen group healthcheck maxtries

Description Resets the maximum number of healthcheck retries to the default values for one or all ActiveN groups.

This command does not take effect until after a `write` operation.

Syntax `clear activen group <name | all> healthcheck maxtries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen group session timeout

Description Resets the timeout settings to the default values for one or all ActiveN groups.

This command does not take effect until after a `write` operation.

Syntax `clear activen group <name | all> session timeout <ackwait | active | closewait>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen group stats

Description Clears the statistics for an ActiveN group.

This command does not take effect until after a `write` operation.

Syntax

```
clear activen group <name | all> stats
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear activen stats

Description Clears overall ActiveN statistics.

This command does not take effect until after a `write` operation.

Syntax

```
clear activen stats
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

clear admin Commands

Use the `clear admin` commands to clear admin settings such as TFTP, SCP, Syslog, E-Mail, interface, TSDump, TCPDump, and logging.

clear admin email defaultmailto

Description Clears the default email address for sending logs.

This command does not take effect until after a `write` operation.

Syntax

```
clear admin email defaultmailto
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin interface

Description Clears the administrator Ethernet interface settings. Clearing the admin interface also clears the admin VIP.

This command does not take effect until after a `write` operation.

Syntax `clear admin interface`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log <mailto1 | mailto2>

Description Clears the first or second mail-to address for log messages.

This command does not take effect until after a `write` operation.

Syntax `clear admin log <mailto1 | mailto2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method apprules memory level

Description Clears the log level for apprules logs sent to memory.

Syntax `clear admin log method apprules memory level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method apprules syslog facility

Description Clears the syslog facility for apprules logs.

Syntax `clear admin log method apprules syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method apprules syslog level

Description Clears the log level for apprules logs sent to a syslog server.

Syntax `clear admin log method apprules syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method audit syslog facility

Description Clears the syslog facility for audit logs.

Syntax `clear admin log method audit syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method audit syslog level

Description Clears the log level for audit logs sent to a syslog server.

Syntax `clear admin log method audit syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method health memory level

Description Clears the log level for scriptable health logs sent to memory.

Syntax `clear admin log method health memory level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method health syslog facility

Description Clears the syslog facility for scriptable health logs.

Syntax `clear admin log method health syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method health syslog level

Description Clears the log level for scriptable health logs sent to a syslog server.

Syntax `clear admin log method health syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method system email level

Description Clears the log level for system logs sent by email.

Syntax `clear admin log method system email level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method system syslog facility

Description Clears the syslog facility for system logs.

Syntax `clear admin log method system syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin log method system syslog level

Description Clears the log level for system logs sent to a syslog server.

Syntax `clear admin log method system syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin remoteauth ldap

Description Clears the LDAP server settings.

This command does not take effect until after a `write` operation.

Syntax `clear admin remoteauth ldap <base-dn | bind password | bind user-dn | server <1 | 2> ip | uid>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear admin remoteauth radius server

Description Clears the key used for the RADIUS server(s) or the IP address for RADIUS server 1 or RADIUS server 2.

This command does not take effect until after a `write` operation.

Syntax `clear admin remoteauth radius server <1 | 2> ip | <key>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear admin remoteauth userrole

Description Resets the default role for remote users (default is user).

This command does not take effect until after a `write` operation.

Syntax `clear admin remoteauth userrole`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear admin scp server

Description Clears the server name or IP address for SCP transfers.

This command does not take effect until after a `write` operation.

Syntax `clear admin scp server`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin scp username

Description Clears the username used for SCP transfers.

This command does not take effect until after a `write` operation.

Syntax `clear admin scp username`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin snmp trap host

Description Clears the first or second SNMP trap host.

This command does not take effect until after a `write` operation.

Syntax `clear admin snmp trap host <1 | 2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin syslog facility

Description Sets the Syslog facility settings back to the default value.

This command does not take effect until after a `write` operation.

Syntax `clear admin syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin syslog host ip

Description Clears the first or second Syslog host IP address.

This command does not take effect until after a `write` operation.

Syntax `clear admin syslog host <1 | 2> ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin tcpdump

Description Clears the first or second email address for TCPDump.

This command does not take effect until after a `write` operation.

Syntax `clear admin tcpdump <mailto1 | mailto2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin tftp server

Description Clears the TFTP server.

This command does not take effect until after a `write` operation.

Syntax `clear admin tftp server`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin tsdump

Description Clears the first or second email address for TSDump.

This command does not take effect until after a `write` operation.

Syntax `clear admin tsdump <mailto1 | mailto2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear admin webui ssl keypass

Description Clears the SSL keypass (pass phrase) for accessing the WebUI using SSL.

This command does not take effect until after a `write` operation.

Syntax `clear admin webui ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear authentication cache

Description Use the `clear authentication` command to clear the authentication cache.

This command does not take effect until after a `write` operation.

Syntax `clear authentication cache`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

clear cache

Description Clear statistics and cached objects for a named cache or all caches. Use the stats option to clear just the statistics.

This command does not take effect until after a `write` operation.

Syntax `clear cache <name | all> [stats]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

clear cluster aaa authentication Commands

Use the `clear cluster <name>` aaa authentication commands to clear cluster authentication options or certfiles.

clear cluster aaa authentication ldap base-dn

Description Clears the root Distinguished Name (DN) user for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication ldap base-dn`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication ldap gid

Description Clears the Group ID used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication ldap gid`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication ldap server

Description Clears the LDAP server IP address. N is either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication ldap server <N> ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication ldap ssl cacertfile

Description Clears the cacert file for SSL.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication ldap ssl cacertfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication ldap uid

Description Clears the User ID used for the cluster authentication.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication ldap uid`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication radius server

Description Clears the IP address of the RADIUS server for the cluster. N is either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication radius server <N> ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication radius server key

Description Clears the authentication key for the RADIUS server used by the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication radius key`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication realm

Description This command is used to reset the realm name that is displayed in the login pop-up dialog box.

This command does not take effect until after a `write` operation.

Syntax `clear cluster aaa authentication realm`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication redirect host

Description Resets the redirect host to its default value.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication redirect host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication redirect protocol

Description Resets the redirect protocol to its default value.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication redirect protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication redirect url

Description Resets the redirect URL to its default value.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication redirect url`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication response text

Description Clears the response string added to HTTP401 responses.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication response text`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster aaa authentication sso domain

Description Clears the Single Sign-On (SSO) domain for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> aaa authentication sso domain`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) AAA Authentication

clear cluster apprule ruleset

Description Clears the Application Rules filename setting for a cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> apprule ruleset`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Overdrive Application Rules

clear cluster apprule

Description Clears the Application Rules statistics for one or all clusters.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <n | all> apprule stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Overdrive Application Rules

clear cluster cache

Description Disassociates the cached objects from a cluster so the cluster has no cache.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> cache`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

clear cluster compression

Description Resets the compression settings for a cluster to the global settings.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> compression <cmt <1 | 2 | 3> | flushthreshold >`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster customiplogheader

Description Resets the logging HTTP header for a cluster to the global setting.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> customiplogheader`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster description

Description Clears a description associated with a cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster forwardclientcert headername

Description Resets the client SSL certificate for a cluster to the global setting.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> forwardclientcert headername`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster health request

Description Clears the string or size requirement for a successful health check.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> health request <size | string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

clear cluster listen ssl Commands

Use these commands to clear a CA certificate file, CA CRL file, a CA trusted certificate, an ephemeral key filename, or ephemeral key password.

clear cluster listen ssl certfile

Description Clears the listen-side SSL certificate file for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl cipherfile

Description Clears the listen-side SSL cipher file for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl cipherfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl clientauth cacertfile

Description Clears the value of the CA certificate file, making this field empty.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl clientauth cacertfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl clientauth cacrlfile

Description Clears the value of the CA CRL file, making this field empty.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl clientauth cacrlfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl clientauth catrustfile

Description Clears the value of the CA Trusted file, making this field empty.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl clientauth catrustfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl ephkeyfile

Description Clears the listen-side SSL ephemeral key file for the cluster

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl ephkeyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl ephkeypass

Description Clears the listen-side SSL ephemeral key password for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl ephkeypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl keyfile

Description Clears the listen-side SSL keyfile for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster listen ssl keypass

Description Clears the listen-side SSL keypass (pass phase) for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> listen ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster sacompat advanced url

Description Clears the URLs defined for the DX to operate with the Juniper Secure Access SSL VPN (SA) solution.You cannot clear all three URLs. URL must remain configured with its default value at a minimum.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> sacompat advanced url <1|2|3>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

clear cluster stats

Description Clears the statistics for a cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster sticky clientip entry

Description Clears one or all entries associating client IP addresses with target hosts for the specified cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> sticky clientip entry <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster target Commands

Use these commands to clear cluster target parameters.

clear cluster target host

Description Clears one or all target hosts for a cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target host <ip:port | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster target localip

Description Removes the local IP setting for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target localip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear cluster target name

Description Clears the cluster target name.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target name`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster target ssl certfile

Description Clears the target-side SSL certfile for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster target ssl cipherfile

Description Clears the target-side SSL cipherfile for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target ssl cipherfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster target ssl keyfile

Description Clears the target-side SSL keyfile for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster target ssl keypass

Description Clears the target-side SSL keypass (pass phrase) for the cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> target ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear cluster weblog Commands

Use these commands to configure the Weblog feature.

clear cluster weblog batch copy time

Description Clears one of the three times for the Web Log to be transmitted to the configured Syslog server.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> weblog batch copy time <1 | 2 | 3>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Statistics

clear cluster weblog batch scp keyfile

Description Clears the (non-password protected) private key.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> weblog batch scp keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Statistics

clear cluster weblog syslog host

Description Clears the Web Log host for a specific cluster.

This command does not take effect until after a `write` operation.

Syntax `clear cluster <name> weblog syslog host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Statistics

clear dns server

Description Clears one or all DNS servers.

This command does not take effect until after a `write` operation.

Syntax `clear dns server [1-3 | all]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear failover stats

Description Clears the general and advanced Unified Failover statistics, including the supported services and the amount of time spent in each mode (master, standby, discovery, and idle).

This command does not take effect until after a `write` operation.

Syntax `clear failover stats [advanced]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

clear forwarder Commands

Use these commands to clear the description, statistics, SSL settings, or target hosts for a forwarder. You can also clear the target address and SSL settings.

clear forwarder description

Description Clears the description associated with a forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear forwarder listen ssl certfile

Description Clears the listen-side SSL certfile for the forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> listen ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl cipherfile

Description Clears the listen-side SSL cipherfile for the forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> listen ssl cipherfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl clientauth

Description Clears the listen-side SSL client authentication parameters.

This command does not take effect until after a `write` operation.

Syntax

```
clear forwarder <name> listen ssl clientauth <cacertfile | cacrlfile |
catrustfile>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl ephkeyfile

Description Clears the listen-side SSL ephemeral key for the forwarder.

This command does not take effect until after a `write` operation.

Syntax

```
clear forwarder <name> listen ssl ephkeyfile
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl ephkeypass

Description Clears the listen-side SSL ephemeral key password (pass phrase) for the forwarder.

This command does not take effect until after a `write` operation.

Syntax

```
clear forwarder <name> listen ssl ephkeypass
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl keyfile

Description Clears the listen-side SSL keyfile for the forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> listen ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder listen ssl keypass

Description Clears the listen-side SSL keypass (pass phrase) for the forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> listen ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

clear forwarder stats

Description Clears the statistics for a forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

clear forwarder sticky clientip entry

Description Clears one or all entries associating client IP addresses with target hosts.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> sticky clientip entry <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear forwarder target host

Description Removes one or all target hosts from a forwarder. This command clears all parameters related to the target hosts.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> target host <ip:port | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear forwarder target localip

Description Removes the local IP setting for the forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> target localip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear forwarder target ssl

Description Clears the target-side SSL certfile, cipherfile, keyfile, or keypass (pass phrase for a forwarder.

This command does not take effect until after a `write` operation.

Syntax `clear forwarder <name> target ssl <certfile | cipherfile | keyfile | keypass>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear fwlb Commands

clear fwlb group target host

Description Clears one or all target hosts from a firewall load-balancing group. This command clears all parameters related to the target hosts.

This command does not take effect until after a `write` operation.

Syntax `clear fwlb group <name> target host <ip|all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

clear fwlb group target host stats

Description Clears all target host statistics associated with a firewall load-balancing group.

This command does not take effect until after a `write` operation.

Syntax `clear fwlb group <name> target host <ip|all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

clear fwlb group session

Description Clears one or all sessions on a given firewall load balancer group.

This command does not take effect until after a `write` operation.

Syntax `clear fwlb group <name|all> session`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

clear fwlb group stats

Description Clears one or all statistics for a specified firewall load-balancing group.

This command does not take effect until after a `write` operation.

Syntax `clear fwlb group <name|all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

clear fwlb group sticky

Description Clears one or all associations between a particular firewall and the specified firewall load balancer group. Traffic from a particular firewall may not be processed by the firewall load balancer and returned to that firewall, potentially causing this traffic to be dropped.

This command does not take effect until after a `write` operation.

Syntax `clear fwlb group <name|all> sticky`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall load balancer

clear gslb Commands

Use these commands to clear Global Server Load Balancing (GSLB) settings.

clear gslb agent encryption key

Description Removes the Nth encryption key for the GSLB agent.

This command does not take effect until after a `write` operation.

Syntax `clear gslb agent encryption key <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb agent stats

Description Clears the GSLB agent statistics.

This command does not take effect until after a `write` operation.

Syntax `clear gslb agent stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb localdns domain

Description Clears the specified DNS records for the local DNS.

This command does not take effect until after a `write` operation.

Syntax `clear gslb localdns domain <a | cname | mx | ns | ptr>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb remotenode encryption key

Description Removes the encryption key for the remote node.

This command does not take effect until after a `write` operation.

Syntax `clear gslb remotenode <name> encryption key`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb remotenode stats

Description Clears the GSLB statistics for the specified remote node.

This command does not take effect until after a `write` operation.

Syntax `clear gslb remotenode <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb resolver group failip

Description Removes the IP address that is sent to the local DNS when all DX nodes in a group are unavailable.

This command does not take effect until after a `write` operation.

Syntax `clear gslb resolver <name> group <name> failip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb resolver group member stats

Description Clears the GSLB statistics for a specific group member.

This command does not take effect until after a `write` operation.

Syntax `clear gslb resolver <name> group <name> member <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb resolver group stats

Description Clears a GSLB group's statistics.

This command does not take effect until after a `write` operation.

Syntax `clear gslb resolver <name> group <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear gslb resolver stats

Description Clears a resolver's statistics.

This command does not take effect until after a `write` operation.

Syntax `clear gslb resolver <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

clear health Commands

Use these commands to remove an IP address from Connectivity Failover Health Check or to clear the statistics for a health script.

clear health remotehost host

Description Removes an IP address from Connectivity Failover health check.

This command does not take effect until after a `write` operation.

Syntax `clear health remotehost host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

clear health script

Description Clears the statistics for the named health script or all health scripts.

This command does not take effect until after a `write` operation.

Syntax `clear health script <script_name | all> [stats]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

clear log Commands

Use these commands to clear entries from the Audit, Apprule, Health, and System logs.

clear log apprule

Description Clears the Application Rule log.

This command does not take effect until after a `write` operation.

Syntax `clear log apprule`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Application Rules

clear log audit

Description Clears the Audit Log.

This command does not take effect until after a `write` operation.

Syntax `clear log audit`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear log health script

Description Clears the Scriptable Health Check Script log.

This command does not take effect until after a `write` operation.

Syntax `clear log health script`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

clear log system

Description Clears the System log.

This command does not take effect until after a `write` operation.

Syntax `clear log system`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear ntp server

Description Clear a specific NTP server or all NTP servers.

This command does not take effect until after a `write` operation.

Syntax `clear ntp server <1-3 | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector Commands

Use these commands to clear redirector options, or the certificate files, passwords, and keyfiles associated with a redirector's SSL traffic.

clear redirector customURL

Description Clears the URL for redirecting.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> customURL`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector description

Description Clears a description from a redirector.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector host

Description Clears the setting for the redirector host.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl certfile

Description Clears the redirector listen SSL certfiles.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> listen ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl cipherfile

Description Clears the redirector listen SSL cipherfiles.

This command does not take effect until after a `write` operation.

Syntax

```
clear redirector <name> listen ssl cipherfile
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl clientauth

Description Clears the redirector listen SSL client authentication parameters.

This command does not take effect until after a `write` operation.

Syntax

```
clear redirector <name> listen ssl clientauth <cacertfile | cacrlfile |
catrustfile>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl ephkeyfile

Description Clears the redirector listen SSL ephemeral keyfiles.

This command does not take effect until after a `write` operation.

Syntax

```
clear redirector <name> listen ssl ephkeyfile
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl ephkeypass

Description Clears the redirector listen SSL ephemeral keypass (pass phrase).

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> listen ssl ephkeypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl keyfile

Description Clears the redirector listen SSL keyfiles.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> listen ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector listen ssl keypass

Description Clears the redirector listen SSL keypass (pass phrase).

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> listen ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear redirector stats

Description Clears the redirector statistics.

This command does not take effect until after a `write` operation.

Syntax `clear redirector <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear server Commands

Use the `clear server` commands to clear server compression, statistics, a custom IP log header, or reverse path entries.

clear server compression

Description Clears server compression options.

This command does not take effect until after a `write` operation.

Syntax `clear server compression`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear server compression cmt

Description Clears Custom Mime Types 1, 2, or 3.

This command does not take effect until after a `write` operation.

Syntax `clear server compression cmt [1 | 2 | 3]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear server customiplogheader

Description Clears the HTTP header for reporting client IPs to the target server.

This command does not take effect until after a `write` operation.

Syntax `clear server customiplogheader`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear server reversepath entry

Description Clears an entry created by reversepath routing. If you have a packet from a gateway that is not your default gateway, you will never get a response unless you configure your routing tables to send the packet back through the right gateway (route). Reversepath does this automatically.

This command does not take effect until after a `write` operation.

Syntax `clear server reversepath entry <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear server stats

Description Clears the server's I/O, HTTP, and SSL statistics.

This command does not take effect until after a `write` operation.

Syntax `clear server stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

clear slb Commands

Use the `clear slb` commands to clear the Server Load Balancer (SLB) settings and statistics.

clear slb failover

The service-specific failover commands are listed in "Service Failover Commands" on page 479. These commands have been replaced by the commands for Unified Failover (refer to "set failover Commands" on page 215).

clear slb group healthcheck interval

Description Resets the healthcheck interval settings to the default values for one or all SLB groups.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name | all> healthcheck interval <down | syn |up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group healthcheck maxtries

Description Resets the maximum number of healthcheck retries to the default values for one or all SLB groups.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name | all> healthcheck maxtries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group session timeout

Description Resets the session timeouts to the default values for one or all SLB groups.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `clear slb group <name | all> session timeout <ackwait | active | closewait>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group stats

Description Clears the statistics for one or all groups.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

clear slb group sticky entry

Description Clears one or all entries associating client IP addresses with target hosts.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name> sticky entry <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group sticky timeout

Description Resets the sticky timeout to the default value for one or all SLB groups.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `clear slb group <name | all> sticky timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group target host

Description Removes the specified target host(s) from one or all groups.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name | all> target host <ip:port | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb group target host <ip:port | all> stats

Description Clears the target host statistics.

This command does not take effect until after a `write` operation.

Syntax `clear slb group <name | all> target host <ip:port | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

clear slb stats

Description Clears all statistics for SLB.

This command takes effect immediately and does not require a `write` operation.

Syntax `clear slb stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer Configuration

clear snat group member

Description Removes one or all members from a Source Network Address Translation (SNAT) group.

This command does not take effect until after a `write` operation.

Syntax `clear snat group <name> member <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Direct Server Return

clear sync group Commands

Use the `clear sync group <name>` commands to clear a synchronization group's description or override file name. Starting with software release 4.1.15, the clear sync group command is disabled on the DX 3670.

clear sync group description

Description Clears the description for the named sync group.

This command does not take effect until after a `write` operation.

Syntax `clear sync group <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear sync group override filename

Description Clears the name for the sync group's override file.

This command does not take effect until after a `write` operation.

Syntax

```
clear sync group <name> override filename
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

clear user role

Description Use the `clear user` command to remove one or more roles from one or all users. This command will not modify the default "admin" user or the user with the administrator's role who is making the changes. The roles are:

- administrator
- network_administrator
- network_operator
- security_administrator
- security_operator
- user
- target_host_operator

This command takes place immediately; no `write` command is needed.

Syntax

```
clear user <username> role <role1 role2   >
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

Examples

```
Clear user bmartino role administrator security_administrator
```

Removes the "administrator" and "security_administrator" roles from user bmartino.

clear vlan Commands

Use the `clear vlan` command to clear virtual LAN parameters.

clear vlan all

Description Clears all tags.

This command does not take effect until after a `write` operation.

Syntax `clear vlan all`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear vlan default

Description Clears the default VLAN.

This command does not take effect until after a `write` operation.

Syntax `clear vlan default`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

clear vlan ip

Description Clears the assignment of a VLAN tag to all packets going to or from one or all IP addresses.

This command does not take effect until after a `write` operation.

Syntax `clear vlan ip <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Example `clear vlan ip 192.168.10.100`

Clears the assignment of a VLAN tag to all the packets going to or from the IP address 192.168.10.100.

clear vlan range

Description Clears the assignment of VLAN tags to packets going from or to this range of IP addresses.

This command does not take effect until after a `write` operation.

Syntax `clear vlan range <startip-endip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Example `clear vlan range 192.168.10.100-192.168.10.200`

Clears the assignment of VLAN tags to all the packets going to or from the range of IP addresses 192.168.10.100 to 192.168.10.200.

clear vlan tag

Description Clears the VLAN with the named tag.

This command does not take effect until after a `write` operation.

Syntax `clear vlan tag <tag>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

cls

Description Use the `cls` command to clear the screen.

Syntax `cls`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

configure

Description Use the `configure` command to rerun the configuration walk-through.

This command does not take effect until after a `write` operation.

Syntax `configure`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

copy Commands

Use the `copy` command to copy configurations, files, and captured TCPDump information.

- Copying configurations from a remote location is equivalent to importing a configuration. This can also be performed by entering the command:

  `import config`

  (for additional information, see “import config” on page 99).

- Copying configurations to a remote location is equivalent to exporting a configuration. This can also be performed by entering the command:

  `export config`

  (for additional information, see “export Commands” on page 92).

- Displaying the CLI commands needed to re-create the configurations can be performed by entering the command:

  ```
  display config
  ```

  (for additional information, see “display config” on page 91).

- To reset all configurations back to factory defaults, enter the command:

  ```
  reset config
  ```

  (for additional information, see “reset config” on page 107).

WARNING: Executing this command resets the network configuration. If you are logged in using Secure Socket Shell (SSH) or WebUI, you will lose contact with the DX.

- To display the contents of a file, enter the command:

  ```
  display file
  ```

  (for additional information, see “display file” on page 91).

- To capture an SSL key or certificate onto a file on the DX, enter the command:

  ```
  capture file
  ```
  (for additional information, see “add user” on page 23).

- In order to use SCP, you must first configure the environment using the commands:

  ```
  set admin scp username <user>
  ```
and
  ```
  set admin scp server <servername>
  ```

copy config

Description Use `copy config` command to:

- Copy configurations from the DX to a remote location or from a remote location to the DX via TFTP or SCP.
- Display the CLI commands needed to re-create the configuration on the terminal screen.
- Reset the configuration to factory defaults

Syntax

```
copy config [tftp://tftp_server/filename| scp://[username@]scp_server/filename|
memory | active | terminal | factory | local filename]
[tftp://tftp_server/filename| scp://[username@]scp_server/filename| memory |
active | terminal | factory | local filename]
```

The format of `< src >` and `< dst >` is:

- Remote location:

  `tftp://tftp_server/filename`

  or

  `scp://[username@]scp_server/filename`

- Local location:
  - memory: Configuration currently stored in memory
  - active: Configurations currently on Flash
  - terminal: The CLI terminal screen
  - factory: The factory default configuration
  - local filename: Creates a named configuration stored locally

Either `< src >` or `< dst >` must be in the memory.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

copy file

Description Use `copy file` command to:

- Display the contents of the file on the terminal screen
- Capture a SSL key or certificate as a file onto the DX

The format of `<src>` and `<dst>` is:

- Local filename
- Remote filename:

`tftp://tftp_server/filename or scp://[username@]scp_server/filename`

- Terminal: the CLI terminal

The following are invalid copy file operations:

- Remote file to the terminal
- Remote file to a remote file

- Terminal to a remote file
- Terminal to the terminal

Syntax

```
copy file [local filename | tftp://tftp_server/filename |
scp://[username@]scp_server/filename | terminal] [local filename |
tftp://tftp_server/filename | scp://[username@]scp_server/filename | terminal]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

copy tcpdump

Description Use the `copy tcpdump` command to send the specified TCPDump file via email (SMTP), SCP, or TFTP as configured in the TCPDump destination.

Syntax

```
copy tcpdump <tcpdumpfile> <tftp://tftp_server/filename |
scp://[username@]scp_server/filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete Commands

Use the `delete` command to delete clusters, forwarders, redirectors, routes, configurations, files, login banners, server load balancers, and users.

delete activen blade

Description Deletes an ActiveN blade specified by the index. Using “all” deletes all blades. This command requires an ActiveN license before it can be used.

This command does not take effect until after a `write` operation.

Syntax

```
delete activen blade <ip | all>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

delete activen group

Description Deletes an ActiveN group. Using “all” deletes all groups. This command requires an ActiveN license before it can be used.

This command does not take effect until after a `write` operation.

Syntax `delete activen group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

delete cache

Description Deletes the named cache. You cannot delete a cache that is being used by a cluster.

This command does not take effect until after a `write` operation.

Syntax `delete cache <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

delete cluster

Description Deletes a specific cluster or all clusters.

This command does not take effect until after a `write` operation.

Syntax `delete cluster <cluster name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete config

Description Deletes a previously saved configuration.

This command does not take effect until after a `write` operation.

Syntax `delete config <saved_config>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete ether subnet

Description Deletes an existing subnet from an interface.

This command does not take effect until after a `write` operation.

Syntax `delete ether <id> subnet <ip> <netmask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete failover peer

Description Deletes one or all remote static peers defined for Unified Failover.

This command does not take effect until after a `write` operation.

Syntax `delete failover peer <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) Unified Failover

delete file

Description Deletes the specified file.

This command takes effect immediately.

Syntax `delete file <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

delete floatingvip

Description Deletes a floating VIP.

This command does not take effect until after a `write` operation.

Syntax `delete floatingvip <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete forwarder

Description Deletes a specific forwarder or all forwarders.

This command does not take effect until after a `write` operation.

Syntax `delete forwarder <forwarder name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete fwlb group

Description Deletes a specific firewall load-balancing group.

This command does not take effect until after a `write` operation.

Syntax `delete fwlb group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete gslb localdns domain

Description Deletes a fully-qualified domain name and all its records.

This command does not take effect until after a `write` operation.

Syntax `delete gslb localdns domain <domain>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

delete gslb remotenode

Description Deletes one or all remote node definitions on a GSLB master.

This command does not take effect until after a `write` operation.

Syntax `delete gslb group <name> remotenode <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

delete gslb resolver

Description Deletes one or all resolvers on a GSLB master.

This command does not take effect until after a `write` operation.

Syntax `delete gslb group <name> resolver <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

delete gslb resolver group

Description Deletes one or all groups on a GSLB master.

This command does not take effect until after a `write` operation.

Syntax `delete gslb resolver <name> group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

delete gslb resolver group member

Description Deletes a member from a GSLB group.

This command does not take effect until after a `write` operation.

Syntax `add gslb resolver <name> group <name> member <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

delete gslb resolver group servicecheck tcp port

Description Removes all or specified ports from the TCP service check.

Syntax `delete gslb resolver [name] group [name] servicecheck tcp port [port | all]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancing

delete health script

Description Deletes a health script configuration node.

This command does not take effect until after a `write` operation.

Syntax `delete health script <script_name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Health Checking

delete loginbanner

Description Deletes a previously set login banner.

This command does not take effect until after a `write` operation.

Syntax `delete loginbanner`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

delete redirector

Description Deletes a specific redirector or all redirectors.

This command does not take effect until after a `write` operation.

Syntax `delete redirector <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete route

Description Deletes one or all routes. Use the show route command to view the current routes (the destination IP address is shown in the first column).

This command does not take effect until after a `write` operation.

Syntax `delete route <destination_ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete slb group

Description Deletes one or all Server Load Balancer (SLB) groups.

This command does not take effect until after a `write` operation.

Syntax `delete slb group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete snat group

Description Deletes a Source Network Address Translation (SNAT) group.

This command does not take effect until after a `write` operation.

Syntax `delete snat group <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete ssh authorized_keys

Description Removes the user's public SSH key from the DX. The user executing this command will have their public SSH key deleted.

Syntax `delete ssh authorized_keys`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

delete sync group

Description Deletes one or all synchronization groups. Starting with software release 4.1.15, the `delete sync group` command is disabled on the DX 3670.

This command does not take effect until after a `write` operation.

Syntax `delete sync group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete sync group member

Description Removes a member from the synchronization group. `<memberid>` is either `<hostname>` or `<ip>`. Starting with software release 4.1.15, the `delete sync group` command is disabled on the DX 3670.

This command does not take effect until after a `write` operation.

Syntax `delete sync group <name> member <memberid>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

delete tcpdump

Description Deletes one or all TCP dump files from the DX.

This command takes place immediately; no `write` command is needed.

Syntax `delete tcpdump [tcpdumpfile | all]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

delete user

Description Deletes one or all users from the DX.

This command takes place immediately; no `write` command is needed.

Syntax `delete user <user_name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

delete user ssh authorized_keys

Description Removes the specified user's public SSH key from the DX.

Syntax `delete user <name> ssh authorized_keys`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

display Commands

Use the `display` commands to display the CLI commands required to create the current configuration or contents of a file.

display config

Description Displays the CLI commands to re-create the current working configuration.

Syntax `display config`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

display file

Description Displays the contents of the specified file.

Syntax `display file <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

display loginbanner

Description Displays the banner in its raw form. Substitution strings are shown in their normal form (`%h`) instead of the substitution form (hostname).

Syntax `display loginbanner`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

display users

Description Displays the commands needed to recreate user accounts.

Syntax `display users`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

exit

Description Use the `exit` command to end a session (same as the `quit` command).

Syntax `exit`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

export Commands

Use the `export` commands to export configurations and user accounts from the DX to a remote server via TFTP or SCP.

Notes:

The format of `<dst>` is:

```
tftp://tftp_server/filename or scp://[username@]scp_server/filename
```

Double quotes must be used if the filename has spaces:

```
“tftp://tftp_server/dx config”
```

The `<scp_server>` name is a host name or an IP address. The `<filename>` is an absolute path of the file where you would like to export the configuration. The directory specified for the filename must exist. The System Snapshot can only be exported to an SCP server.

NOTE: When exporting a configuration or a snapshot, it is a good practice to give the file a name that describes the function and identifies the version.

For example:

```
ex_4.1.B14_ssl_server_8-25-2003
```

The `export config` command exports the actual set commands from the CLI to recreate the configuration, however, it only exports those commands that are

allowed by the current role. The `export config` operation does not export the following information:

- `Set` commands take effect immediately. These commands include the state of the various services:
  - Server
  - SSH Service
  - Telnet Service
  - SNMP Service
  - Web User Interface Service
- Administrative passwords
- All SSL private keys, key passwords, certificates and self-signed certificates
- User accounts

Because the `export config` command does not cover these cases, the `export audit`, `export log`, `export ruleset`, and `export users` commands were added.

Note that to use SCP, you must first configure the environment using the commands:

```
set admin scp username <user> and set admin scp server <servername>
```

export cluster stats history

Description Exports statistics for one or all clusters via TFTP or SCP.

Syntax

```
export cluster <name | all> stats history <dst>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

export config

Description Exports a configuration from the DX to a remote location via TFTP or SCP.

Syntax

```
export config <dst>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

export log apprule

Description Exports the Apprule Event log from the DX to a remote location via SCP (only).

Syntax `export log apprule <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Application Rules

export log audit

Description Exports the Audit Event log from the DX to a remote location via SCP (only).

Syntax `export log audit <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

export log health script

Description Exports the Health Script log from the DX to a remote location via TFTP or SCP.

Syntax `export log health script <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Health Checking

export log system

Description Exports the System Event log from the DX to a remote location via SCP (only).

Syntax `export log system <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

export ruleset

Description Exports the OverDrive AppRule ruleset from the DX to a remote location via TFTP or SCP.

Syntax `export ruleset <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Application Rules

export snapshot system

Description Exports a system snapshot from the DX to a remote location via SCP (only).

Syntax `export snapshot system <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

export users

Description Exports user accounts from the DX to a remote location via TFTP or SCP.

Syntax `export users <dst>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

gen Commands

Use the `gen` commands to generate an SSL private key, an SSL certificate signing request, or an SSL self-signed certificate. The `gen csr`, `gen key`, and `gen ssc` commands are disabled on the DX 3650-FIPS.

You will be prompted for information such as country, state, department, etc. for the certificate. For additional information, see the "Setting-up the DX for SSL Traffic" chapter of the *Installation and Administration Guide for DXOS*.

This command does not take effect until after a `write` operation.

gen cac

Description Generates a self-signed CA Root Certificate.

This command does not take effect until after a `write` operation.

Syntax

```
gen cac
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

gen csr

Description Generates an SSL Certificate Signing Request. Input to the command is a 1024-bit RSA private key file, and the output is a CSR file. [`key_file`] and [`csr_file`] are optional parameters and will be prompted on the command line, if not provided.

This command does not take effect until after a `write` operation.

Syntax

```
gen csr [key file] [csr file]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

gen key

Description Generates a 1024-bit RSA SSL private key.

This command does not take effect until after a `write` operation.

Syntax

```
gen key <key file>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

gen ssc

Description Generates an SSL Self-Signed Certificate. Input to the command is a 1024-bit RSA private key file, and the output is a CSR file.

This command does not take effect until after a `write` operation.

Syntax

```
gen ssc <key file> <ssc file>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

halt

Description The `halt` command provides a graceful mechanism for powering down the DX. This command reduces the possibility of file system corruption. After you enter the `halt` command, a confirmation message is displayed:

```
Warning: This device will now shutdown.
Are you sure you want to continue (y/n)? [n] y

Shutting Down. Please wait 30 seconds before unplugging the power cord once the
DX is halted.
```

Syntax

```
halt
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

help

Description Enter the `help` command by itself to display a description of the top high-level commands. Enter `help` before a command to view a list of all sub-commands.

Syntax

```
help [sub-command]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

history

Description Use the `history` command to display the command history.

Syntax

```
history
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

import Commands

Use the `import` commands to import configurations and user accounts to the DX via TFTP or SCP.

The `import config` and `import license` commands require a `write` operation in order to have the changes take effect. In addition, `export config` operations do not export user accounts. Use `export users` to export user accounts.

The format of `<src>` is:

```
tftp://tftp_server/filename
or
scp://[username@]scp_server/filename
```

Double quotes must be used if the filename has spaces. For example:

```
“tftp://tftp_server/dx config”
```

It is important to note that the SSL keys and certificates are not exported during an `export config` operation. When importing a configuration, you must either make sure that the required SSL keys and certificates are already installed on the DX, or install them before use.

import config

Description Imports a configuration to the DX from a remote location via TFTP or SCP.

This command does not take effect until after a `write` operation.

Syntax `import config <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

import health certfile

Description Imports a certificate file for scriptable health checking to the DX from a remote location via TFTP or SCP. This is required for LDAP over TLS health check.

This command does not take effect until after a `write` operation.

Syntax `import health certfile <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Health Checking

import health script

Description Imports a license to the DX from a remote location via the TFTP or SCP.

This command does not take effect until after a `write` operation.

Syntax `import health script <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Health Checking

import license

Description Imports a license to the DX from a remote location via TFTP or SCP.

This command does not take effect until after a `write` operation.

Syntax `import license <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

import ruleset

Description Imports an AppRule ruleset onto the DX from a remote location via the TFTP or SCP.

The `import ruleset` command takes effect immediately, and does not require a `write` operation. The ruleset is checked for correct syntax and then saved on the device.

Syntax `import ruleset <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Application Rules

import snapshot system

Description Imports a system snapshot onto the DX from a remote location via SCP (only).

This command does not take effect until after a `write` operation.

Syntax `import snapshot system <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

import ssh authorized_keys

Description Allows any user to import their own public SSH key to the DX appliance.

Syntax `import ssh authorized_keys [path]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

import user ssh authorized_keys

Description Imports the public SSH key for a specific user. The file you import will be renamed to authorized_keys on the DX appliance.

Syntax `import user [name] ssh authorized_keys [path]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

import users

Description Imports user accounts to the DX from a remote location via TFTP or SCP.

The `import users` command takes effect immediately, and does not require a `write` operation.

Syntax `import users <src>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

install

Description

Use the `install` command to download and install new firmware to a non-active partition. The `install` procedure preserves the current version of the firmware and downloads the firmware to the non-active partition. The TFTP or SCP server and the filename to install from must be set as:

```
set admin tftp server <tftp server> or
set admin scp server <scp server>
set admin scp username <scp user>
set admin upgrade filename <pac file filename>
```

If your active partition is currently partition 1, the `install` command will install the new firmware into partition 2. This lets you test the new firmware and revert to the original firmware stored in partition 1, if required.

The `install` operation will preserve the following information:

- SSH keys
- User names and passwords for the administrative users
- Generated certificates
- Network settings, including static routes
- AppRule rulesets (on appliances that have an OverDrive license)

The `install` operation also allows the option to preserve the following configuration settings. On first boot to a new partition, you can choose to import these configuration settings:

- User names and passwords for all users
- Network settings, including static routes and admin interface bindings
- SSL keys and certificates
- Current (active) server configuration
- State of the services, including:
  - Server status
  - Telnet
  - SSH
  - SNMP
  - WebUI

After the `import` operation, you will be prompted to save the configurations using the `write` operation. Admin services (e.g., server, WebUI, SSH, etc.) will also be

prompted to start accordingly, based upon their state before the `install` operation was executed.

NOTE: During an install, the configuration files are copied to the non-active partition. If you reboot to the alternate partition immediately, then the most recent configuration files are used, and no problems should be encountered.

However, you may choose to install the software, and then reboot the DX at a later time to limit network impact. If changes are made to the configuration between the install time and the reboot time, the configuration files on the alternate boot partition are no longer current. You must then do another install just before rebooting the unit in order to have updated configuration files on the alternate boot partition.

Syntax `install`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

list Commands

Use the `list` commands to display a list of saved configurations or user files on the DX.

list config

Description Displays the list of saved configurations on the DX.

Syntax `list config`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

list file

Description Displays the list of user files (certs and keys) stored on the DX.

Syntax `list file`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

list tcpdump

Description Displays the TCPDump file as configured in the TCPDump destination.

Syntax `list tcpdump`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

netstat Commands

Description Use the `netstat` command to show network statistics. These statistics include active internet connection information such as send and receive queues, local and foreign addresses, and states.

`netstat` shows all network statistics.

netstat N

Description Where N is an integer, this command shows network statistics every N seconds.

Syntax `netstat N`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

netstat -a

Description Shows active connections.

Syntax `netstat -a`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

netstat -s

Description Shows network statistics.

Syntax `netstat -s`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

netstat -r

Description Shows Routing Tables.

Syntax `netstat -r`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

ping

Description Use the `ping` command to ping another network node. The following option may be entered after the ping command:

`<IP Address> | <DNS name>`

This command is typically used in troubleshooting and during installation. Common tasks are to ping the target host or the default gateway to verify that the configuration used at the time of installation was correct.

Syntax `ping`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

quit

Description Use the `quit` command to end a CLI session (same as the `exit` command).

Syntax

```
quit
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

reboot

Description Use the `reboot` command to reboot the DX.

Syntax

```
reboot
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

reload

Description Use the `reload` command to back out your configuration changes before a `write` operation. This command discards all changes since the last `write`.

Syntax

```
reload
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X			

Mode(s) Global Configuration

reset config

Description

Use the `reset config` command to reset the DX to factory settings.

Connectivity will be lost if you are connected to the DX remotely. You must set the appropriate network settings prior to the `write` operation if you want to have remote access after `reset config` and `write` operations.

You do not have to perform a `write` operation after the `reset config` command to have the changes take effect. Instead, a warning message will be displayed as follows:

```
dx% reset config
Executing this command will reset all configurations, including network
settings. If you continue, you will need to connect to the console (serial) port
to access the box again.
Are you sure you want to continue (y/n)? [y]
```

Resetting the DX to the factory default settings does not delete the user accounts. To delete all user accounts, use the command `delete user all`.

Syntax

```
reset config
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s)

Global Configuration

Chapter 3
Set Commands

This chapter describes all the set commands for the administrative function and the various DX features, such as ActiveN, clusters, SLB, and GSLB.

set activen Commands

Use the `set activen` command to disable or enable the ActiveN feature, or to change ActiveN parameters. Note that ActiveN requires an ActiveN license.

set activen

Description Enables or disables the ActiveN feature. When disabled is selected, the switch is stopped and all configuration information is deleted (only from the Kernel, not from the configuration file) (default is disabled).

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set activen [disabled* | enabled]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen advanced burst_max

Description Sets the maximum number of timed out sessions that are purged in one timer interval. Setting `burst_max` to zero purges all timed-out sessions in one timer cycle (default is 7,000).

This command does not take effect until after a `write` operation.

Syntax `set activen advanced burst_max <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen advanced policy

Description Sets the switching policy to round-robin or least connection (default is roundrobin).

This command does not take effect until after a `write` operation.

Syntax

```
set activen advanced policy <leastconns | roundrobin>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen advanced reset

Description When active sessions are purged, a reset can be sent to the client and/or server to indicate that the connection has been terminated. This command is used to disable or enable sending of resets to the client or server (default is enabled).

This command does not take effect until after a `write` operation.

Syntax

```
set activen advanced reset <client | server> <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen advanced synflood_protect

Description ActiveN operates in DSR mode, and cannot track if the three-way TCP handshake completed successfully. To protect itself from an attack, the ActiveN purges a connection if the client does not send the final ACK for the handshake.

The `synflood_protect` option is used to enable protection against syn flood attacks (default is enabled).

This command does not take effect until after a `write` operation.

Syntax

```
set activen advanced synflood_protect <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen blade <hardpaused | softpaused | unpaused>

Description Halts or resumes client traffic to one or all DX blades, A “hard” pause terminates all existing traffic, while a “soft” pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set activen blade <ip | all> <hardpaused | softpaused | unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Global Configuration

set activen cleaning_interval

Description The ActiveN switch uses a timer to purge expired sessions. The `cleaning_interval` option is used to set the interval between purges (default is 13 seconds).

This command does not take effect until after a `write` operation.

Syntax

```
set activen advanced cleaning_interval <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen failover

The service-specific failover commands are listed in “Service Failover Commands” on page 479. These commands have been replaced by the commands for Unified Failover (refer to “set failover Commands” on page 215).

set activen group advanced burst_max

Description Sets the maximum number of timed out sessions that are purged in one timer interval for the specified group. Setting `burst_max` to zero purges all timed-out sessions in one timer cycle (default is 7,000).

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> advanced burst_max <number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group advanced policy

Description Sets the switching policy for the specified group to round-robin or least connection (default is roundrobin).

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> advanced policy <leastconns | roundrobin>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group advanced reset

Description Disables or enables the sending of resets to the client or server when active sessions are purged (default is enabled).

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> advanced reset <client | server> <disabled |
enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group advanced synflood_protect

Description Enables or disables the purging of a connection if the client does not send the final ACK in the three-way TCP handshake. The `synflood_protect` option is used to enable protection against SYN flood attacks (default is enabled).

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> advanced synflood_protect <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group blade

Description Used to add a blade as a member of a group. Using the keyword “all” in the group argument results in the blade being added to all the groups. Similarly using “all” in the blade argument results in adding all the blades into the group.

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> blade <ip | all>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) ActiveN

set activen group blade <hardpaused | softpaused | unpaused>

Description Halts or resumes client traffic to one or all DX blades in one or all groups, A “hard” pause terminates all existing traffic; a “soft” pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set activen group <name | all> blade <ip | all> <hardpaused | softpaused |
unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Global Configuration

set activen group <hardpaused | softpaused | unpaused>

Description Halts or resumes client traffic to the blades in one or all groups, A “hard” pause terminates all existing traffic; a “soft” pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set activen group <name | all> <hardpaused | softpaused | unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set activen group healthcheck interval

Description Overrides the global health check intervals for one or all groups.

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> healthcheck interval <down | syn | up> <seconds>
```

- `down`: Number of seconds a blade must be unresponsive before it is taken out of rotation (default is 20).
- `syn`: Number of seconds between consecutive health probes when no response is received (default is 10).
- `up`: Number of seconds a blade has to respond to the health check probe before it is considered unresponsive (default is 45 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group healthcheck maxtries

Description Overrides the global ActiveN value for maximum number of health check tries for one or all groups (default is 3).

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> healthcheck maxtries <number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group session timeout

Description Overrides the global purge timers for idle sessions for one or all groups.

These commands do not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> session timeout <ackwait | active | closewait>
<seconds>
```

- `ackwait`: Three way TCP handshake has not completed (default is 10 seconds).
- `active`: Active sessions (default is 100 seconds).
- `closewait`: Sessions terminated by the client (default is 25 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen group sticky

Description Enables or disables the Client IP Sticky feature, where the load balancer selects the same server for multiple TCP connections from the same client.

The command `set activeN sticky timeout` is not per group, but rather it is a global command that affects all the groups.

This command does not take effect until after a `write` operation.

Syntax

```
set activen group <name | all> sticky <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) ActiveN

set activen group sticky failover

Description Enables or disables sticky failover for the specified ActiveN group. When Unified Failover is also enabled, the standby DX takes on communications for the ActiveN group.

These commands do not take effect until after a `write` operation.

Syntax `set activen group <name> sticky failover <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) ActiveN

set activen healthcheck interval

Description Sets the global health check intervals for ActiveN.

This command does not take effect until after a `write` operation.

Syntax `set activen healthcheck interval <down | syn | up> <seconds>`

- `down`: Number of seconds a blade must be unresponsive before it is taken out of rotation (default is 20).
- `syn`: Number of seconds between consecutive health probes when no response is received (default is 10).
- `up`: Number of seconds a blade has to respond to the health check probe before it is considered unresponsive (default is 45 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen healthcheck maxtries

Description Sets the global ActiveN value for maximum number of health check tries before giving up (default is 3).

This command does not take effect until after a `write` operation.

Syntax `set activen healthcheck maxtries <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen max_blades

Description Sets the maximum number of blades in the system (1 to the licensed limit). The `max_blades` option can be set only when ActiveN is disabled.

This command does not take effect until after a `write` operation.

Syntax `set activen max_blades <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen session timeout

Description Sets the global purge timers for idle sessions.

These commands do not take effect until after a `write` operation.

Syntax `set activen session timeout <ackwait | active | closewait> <seconds>`

- `ackwait`: Three way TCP handshake has not completed (default is 10 seconds).
- `active`: Active sessions (default is 100 seconds).
- `closewait`: Sessions terminated by the client (default is 25 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set activen sticky timeout

Description Sets the timeout value for client IP sticky. The default value is 120 minutes, the minimum is one minute and the maximum is 30 days.

These commands do not take effect until after a `write` operation.

Syntax `set activen sticky timeout <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN

set admin Commands

The set admin commands are used to set administrator configuration options.

set admin cli sessionExpireTime

Description Sets the time out for the CLI session. If no activity occurs before this time, the user is logged out. Setting the `sessionExpireTime` to zero causes the session to never expire. The default = 600 seconds.

Syntax `set admin sessionExpireTime <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin email defaultmailto

Description A default address is used when email addresses are not set. Specific email addresses for log, TCPDump and TSDump, if set, will override the default email address.

This command does not take effect until after a `write` operation.

Syntax `set admin email defaultmailto <default address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin email from

Description The sender's address.

This command does not take effect until after a `write` operation.

Syntax `set admin email from <from address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin email server

Description The IP address or host name for the SMTP server.

This command does not take effect until after a `write` operation.

Syntax `set admin email server <smtp server>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin interface ether

Description Sets the Ethernet interface to use for administration traffic. <N> = 0, 1, 2,...N. The specified interface will support SSH, Telnet, SNMP, the Web UI, and configuration synchronization (SOAP).

This command does not take effect until after a `write` operation.

Syntax `set admin interface ether <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log Commands

Description Use the `set admin log` command to set parameters for logging to various destinations, including the memory of the DX, email, and the Syslog.

The severity levels are in the following order:

- EMERG: Highest level
- ALERT: Lowest level

If you set your alert level to ALERT, you will get both EMERG and ALERT notices. If you set your alert level to EMERG, you will only get EMERG notices.

If neither the `mailto1` or the `mailto2` addresses are set, the address set using the `set admin email` command will be used. For additional information, see "set admin email defaultmailto" on page 118.

These commands do not take effect until after a `write` operation

set admin log

Description Disables or enables the logging function.

This command does not take effect until after a `write` operation.

Syntax

```
set admin log <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log mailto1

Description First email address where the log should be sent.

This command does not take effect until after a `write` operation.

Syntax

```
set admin log mailto1 <first email address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log mailto2

Description Second email address where the log should be sent.

This command does not take effect until after a `write` operation.

Syntax

```
set admin log mailto2 <second email address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method apprules memory level

Description Sets the log level for apprule logs sent to memory. Sends a log message to memory when an event greater than or equal to the selected level occurs.

This command does not take effect until after a `write` operation.

Syntax `set admin log method apprules memory level [ALERT | EMERG]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method apprule syslog facility

Description Sets the syslog facility for apprule logs.

Syntax `set admin log method apprules syslog facility <LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2 | LOG_LOCAL3 | LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method apprule syslog level

Description Sets the log level for apprule logs sent to a syslog server. Sends a log message to the syslog server when an event greater than or equal to the selected level occurs.

This command does not take effect until after a `write` operation.

Syntax `set admin log method apprules syslog level [ALERT | EMERG]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method audit showcmd

Description Disables or enables the logging of `show` commands entered on the CLI in the audit log. By default, the show commands are excluded (disabled).

The settings made by this command will only take effect after a write operation. The show commands will only be logged once a `write` operation has been performed.

Syntax

```
set admin log method audit showcmd <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method audit syslog facility

Description Sets the syslog facility for audit logs.

Syntax

```
set admin log method audit syslog facility <LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2
| LOG_LOCAL3 | LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method audit syslog level

Description Sets the log level for audit logs sent to a syslog server. Sends a log message to the syslog server when an event greater than or equal to the selected level occurs.

Syntax

```
set admin log method audit syslog level [ALERT | EMERG]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method health memory level

Description Sets the log level for scriptable health logs sent to memory.

Syntax

```
set admin log method health memory level <info | ???>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method health syslog facility

Description Sets the syslog facility for scriptable health logs.

Syntax

```
set admin log method health syslog facility <LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2
| LOG_LOCAL3 | LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method health syslog level

Description Sets the log level for scriptable health logs sent to a syslog server.

Syntax

```
set admin log method health syslog level <info>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method system email level

Description Sets the log level for system logs sent by email. Sends a log message to the configured email address(es) when an event greater than or equal to the selected level occurs.

This command does not take effect until after a `write` operation.

Syntax
```
set admin log method system email level <ALERT | EMERG>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method system memory level

Description Sets the log level for system logs sent to memory. Sends a log message to memory when an event greater than or equal to the selected level occurs. The default is ALERT.

This command does not take effect until after a `write` operation.

Syntax
```
set admin log method system memory level <ALERT | EMERG>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method system syslog facility

Description Sets the syslog facility for system logs.

Syntax
```
set admin log method system syslog facility <LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2
| LOG_LOCAL3 | LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin log method system syslog level

Description Sets the log level for system logs sent to a syslog server. Sends a log message to the configured Syslog host(s) when an event greater than or equal to the selected level occurs.

This command does not take effect until after a `write` operation.

Syntax `set admin log method system syslog level <ALERT | EMERG>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin remoteauth Commands

Use the set admin remoteauth commands to configure remote authorization.

set admin remoteauth ldap base-dn

Description Sets the Distinguished Name (DN) of the node in the LDAP Directory Information Tree under which the users have to be searched.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap base-dn <base-dn>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap bind password

Description Sets the password for the LDAP admin user.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap bind password <password>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap bind user-dn

Description Sets the Distinguished Name (DN) of the LDAP admin user.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap bind userdn <user-dn>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap server <1 | 2> ip

Description Sets the IP address for the LDAP server 1 or LDAP server 2.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap server <1 | 2> ip <ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap server <1 | 2> port

Description Sets the port for the LDAP server 1 or LDAP server 2.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap server <1 | 2> port <port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap uid

Description Sets the attribute name that uniquely identifies the user in LDAP database.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap uid <uid>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth ldap version

Description Sets the version of LDAP used by the LDAP servers.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth ldap version <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth protocol

Description Sets the authentication protocol to use for Administrator Remote Authentication.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth protocol <ldap | radius>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth radius server <1 | 2> ip

Description Sets the IP address for the RADIUS server 1 or RADIUS server 2.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth radius server <1 | 2> ip <ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth radius server <1 | 2> port

Description Sets the port for the RADIUS server 1 or RADIUS server 2.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth radius server <1 | 2> port <port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth radius server key

Description Sets the RADIUS server password.

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth radius server key <key>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth radius server retries

Description Sets the maximum number of times the DX resends authentication requests when the RADIUS server does not respond (default is 3).

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth radius server retries <count>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth radius server timeout

Description Sets the number of seconds the DX waits for a response from the RADIUS server (default is 10).

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth radius server timeout <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth status

Description Disables or enables Administrator Remote Authentication (disabled by default)

This command does not take effect until after a `write` operation.

Syntax `set admin remoteauth status [disabled* | enabled]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin remoteauth userrole

Description Sets the default role for remote users (default is user).

This command does not take effect until after a `write` operation.

Syntax

```
set admin remoteauth userrole <role>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set admin scp Commands

Description Use the `set admin scp` commands to configure the SCP server and username, and to import and export user information.

The settings made by this command will only take effect after a `write` operation. The SCP server or TFTP server can be used for the following operations:

- Upgrading the firmware
- Importing and exporting configurations
- Exporting the audit trail
- Exporting the event log
- Sending the TCPDump data captured.
- Sending the Technical Service Dump (TSDump) data to the Juniper Networks Support organization

Syntax

```
set admin scp
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

set admin scp server

Description Configures the SCP server IP address or hostname.

This command does not take effect until after a `write` operation.

Syntax

```
set admin scp server <hostname | ip address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin scp username

Description Configures the username to use for the SCP operation.

This command does not take effect until after a `write` operation.

Syntax `set admin scp username <scp username>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp Commands

Use the `set admin snmp` command to set the SNMP configuration. Setting the SNMP service up or down takes effect immediately.

The SNMP agent supports only read operations (no write operations).

set admin snmp community ip

Description Sets the network to allow SNMP connections.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp community ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp community name

Description Sets the SNMP `read`-only community name.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp community name <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp community netmask

Description Sets the netmask to allow SNMP connections from the specified network.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp community netmask <netmask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp contact

Description Sets the SNMP system contact (MIB II).

This command does not take effect until after a `write` operation.

Syntax `set admin snmp contact <contact>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp

Description Disables or enables SNMP support (enabled by default).

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin snmp <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp location

Description Sets the SNMP system location (MIB II).

This command does not take effect until after a `write` operation.

Syntax `set admin snmp location <location>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin snmp trap

Description Enables or disables sending authentication-failure, enterprise-specific, or generic SNMP traps (all are disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap <authfailure | enterprise | generic > <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin snmp trap host <1 | 2> community

Description Defines the community string for each trap host.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap host <1 | 2> community <community string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin snmp trap host <1 | 2> ip

Description Defines the IP address for each trap host.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap host <1 | 2> ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin snmp trap host <1 | 2> version

Description Defines the SNMP version for each trap host to be either Version 1 or Version 2.

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap host <1 | 2> version <1 | 2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin snmp trap threshold connection

Description Sets the percentage of the maximum number of client-side connections that generates a connection threshold trap (default is 100 %).

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap threshold connection <threshold in %>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin snmp trap threshold loginfail

Description Sets the percentage of login failures that triggers an authentication failure trap (default is 20).

This command does not take effect until after a `write` operation.

Syntax `set admin snmp trap threshold loginfail <threshold in %>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin soap Commands

Description Use the `set admin soap` commands to enable or configure the Simple Object Access Protocol (SOAP) server used for configuration synchronization.

set admin soap <down | up>

Description Disables or enables the SOAP server.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin soap <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set admin soap port

Description Sets the port number for the SOAP server (default is 8070).

This command does not take effect until after a `write` operation.

Syntax `set admin soap port <portnum>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set admin soap ssl certfile

Description Sets the SSL certificate filename for the SOAP server (default is `democert`).

This command does not take effect until after a `write` operation.

Syntax `set admin soap ssl certfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set admin soap ssl keyfile

Description Sets the SSL key file for the SOAP server (default is `demokey`).

This command does not take effect until after a `write` operation.

Syntax `set admin soap ssl keyfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set admin soap ssl keypass

Description Sets the SSL key password for the SOAP server.

This command does not take effect until after a `write` operation.

Syntax `set admin soap ssl keypass <password>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set admin ssh

Description Enables or disables Secure Shell (SSH) access to the DX.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin ssh <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin stats history

Description Enables or disables collection of historical statistics for forwarders, clusters, and target hosts, based on the installed license.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin stats history [up | down]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin syslog Commands

Description Use the `set admin syslog` command to set up one or two Syslog hosts for logging purposes. The Syslog facility is used when the `set admin log syslog` level is set. For additional information, see "set admin log Commands" on page 119.

set admin syslog facility

Description Sets the Syslog facility. The default = LOG_USER.

This command does not take effect until after a `write` operation.

Syntax

```
set admin syslog facility <LOG_LOCAL0 | LOG_LOCAL1 | LOG_LOCAL2 | LOG_LOCAL3 |
LOG_LOCAL4 | LOG_LOCAL5 | LOG_LOCAL6 | LOG_LOCAL7 | LOG_USER>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin syslog host <1 | 2> ip

Description Sets the IP address or hostname for the first or second Syslog server.

This command does not take effect until after a `write` operation.

Syntax

```
set admin syslog host <1 | 2> <ip address | hostname>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin syslog host <1 | 2> port

Description Sets the destination port for the first or second Syslog server (default is 514).

This command does not take effect until after a `write` operation.

Syntax
```
set admin syslog host <1 | 2> port <port>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tcpdump Commands

Description Use the `set admin tcpdump` command to set options relating to TCPDump. Before running the `tcpdump` command, an email address, TFTP server, or SCP server must be specified.

For additional information, see “tsdump” on page 471.

If you are using SCP, you need to set the SCP username using the command `set admin scp username <name>` before entering this command. For additional information, see “set admin scp Commands” on page 130.

set admin tcpdump capturesize

Description The size, from 10 MB to 75 MB, of the admin filesystem for TCPDump files. The default is 10 MB.

This command does not take effect until after a `write` operation.

Syntax
```
set admin tcpdump capturesize
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tcpdump mailto1 <first>

Description The first email address where the TCPDump should be sent.

This command does not take effect until after a `write` operation.

Syntax
```
set admin tcpdump mailto1 <email address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tcpdump mailto2 <second>

Description The second email address where the TCPDump should be sent.

This command does not take effect until after a `write` operation.

Syntax `set admin tcpdump mailto2 <email address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin telnet

Description Use the `set admin telnet` command to turn Telnet access on or off.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin telnet <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin tftp server

Description Use the `set admin tftp` server command to set TFTP server information. The TFTP server can be used for the following operations:

- Upgrading the firmware
- Importing and exporting configurations
- Exporting the audit trail
- Exporting the event log

- Sending the TCP dump data captured
- Sending Technical Service Dump (TSDump) data to the Juniper Networks Support organization.

TFTP transport cannot be used to export Audit Trail or Event logs

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set admin tftp server <hostname | ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tsdump Commands

Description Use the `set admin tsdump` commands to set options relating to technical service dumps. Technical service dump information is used by Juniper Networks personnel to troubleshoot the DX. These parameters must be set before running the `tsdump` command:

- An email address, TFTP server, or SCP server.
- A filename for storing the TSDump, if you are using TFTP or SCP.

If you are using SCP, you need to set the SCP username using the command `set admin scp username <name>` before entering this command. For additional information, see “set admin scp Commands” on page 130.

set admin tsdump filename

Description Sets the remote filename for the TSDump.

This command does not take effect until after a `write` operation.

Syntax `set admin tsdump filename <tsdump filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tsdump mailto1 <first>

Description The first email address where the TSDump should be sent.

This command does not take effect until after a `write` operation.

Syntax `set admin tsdump mailto1 <email address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tsdump mailto2 <second>

Description The second email address where the TSDump should be sent.

This command does not take effect until after a `write` operation.

Syntax `set admin tsdump mailto2 <email address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin tsdump transport

Description Sends TSDump information via selected transport. Any of the options SCP, SMTP, or TFTP can be set, but only one at a time.

This command does not take effect until after a `write` operation.

Syntax `set admin tsdump transport <scp | smtp | tftp>`

- Sends TSDump information via the pre-configured SCP host.
- Sends TSDump information via pre-configured email addresses.
- Sends TSDump information via the pre-configured TFTP host.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin upgrade Commands

Description Use the `set admin upgrade` commands to configure the filename and transport for the DX pac file used to upgrade the firmware. The TFTP server or the SCP server must be configured before the upgrade. To configure the TFTP or SCP server, use the command:

```
set admin tftp server <tftp server>
or
set admin scp server <scp_server>
```

If you are using SCP, you need to set the SCP username using the command `set admin scp username <name>` before entering this command. For additional information, see "set admin scp Commands" on page 130.

set admin upgrade filename

Description Sets the filename of the firmware that will be used for the upgrade.

This command does not take effect until after a `write` operation.

Syntax

```
set admin upgrade filename <filename for the firmware>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin upgrade transport

Description Configures the transport method to use either SCP or TFTP to upgrade or install new firmware.

This command does not take effect until after a `write` operation.

Syntax

```
set admin upgrade transport <scp | tftp>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin vip

Description Use the `set admin vip` command to set the admin IP address.

This command does not take effect until after a `write` operation.

Syntax `set admin vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

set admin webui Commands

Description Use the `set admin webui` command to change settings for the Web User Interface (WebUI).

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

set admin webui <down | up>

Description Enables or disables the Web User Interface.

Syntax `set admin webui <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin webui port

Description Sets the TCP port for accessing the WebUI (default port is 8090).

It is possible to configure WebUI to listen on an IP (10.0.20.0, for example) and use port 8090. At the same time, a cluster of target hosts may be configured to use the same IP and port (10.0.20.0:8090). When a configuration change is made that requires a restart of the multiplexing engine, a WebUI administrator page could be displayed. To prevent this from occurring, you should not use the administrator port as a cluster port.

This command does not take effect until after a `write` operation.

Syntax `set admin webui port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin webui sessionExpireTime

Description Sets the time out for the WebUI session. If no activity occurs before this time, the user must re-authenticate.

This command does not take effect until after a `write` operation.

Syntax `set admin webui sessionExpireTime <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin webui ssl certfile

Description Specifies the SSL certfile for accessing the WebUI over SSL.

This command does not take effect until after a `write` operation.

Syntax `set admin webui ssl certfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin webui ssl

Description Disables or enables Web User Interface access via SSL.

This command does not take effect until after a `write` operation.

Syntax `set admin webui ssl [disabled | enabled]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set admin webui ssl keyfile

Description Specifies the SSL for accessing the WebUI over SSL.

This command does not take effect until after a `write` operation.

Syntax `set admin webui ssl keyfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set admin webui ssl keypass

Description Specifies the SSL key pass phrase for accessing the WebUI over SSL.

This command does not take effect until after a `write` operation.

Syntax `set admin webui ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set boot

Description Use the `set boot` command to set the boot partition (1 or 2) for the next reboot.

This command takes place immediately.

Syntax `set boot <1 | 2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cache Commands

Description Use the `set cache` command to set the parameters for the named 3G cache.

set cache max_objects

Description Sets the total number of objects that can be stored in the named cache. The minimum number is 1024 and the maximum is 32,768.
(The default value is 8,192).

The value for `max_objects` can be abbreviated with a "K" suffix to indicate how many thousands, e.g., 1K = 1000 objects.

This command does not take effect until after a `write` operation.

Syntax `set cache <name> max_objects <integer>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

set cache size

Description The minimum number is 1,048,576 (1 Mbyte) and the maximum is 104,857,600 (100 Mbytes). The default value is 10,485,760 (10 Mbytes). The actual size of the cache can be somewhat larger than this.

The value for `max_objects` can be abbreviated with an "M" suffix to indicate a megabyte, e.g.,1,048,576 bytes = 1 M.

This command does not take effect until after a `write` operation.

Syntax `set cache <name> size <integer>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) 3G Cache

set clock

Description Use the `set clock` command to set the date and time on the DX. If an NTP server is being used, enter set ntp down before using this command.

This command does not take effect until after a `write` operation.

Syntax `set clock <YYYY.MM.DD HH:MM:SS>`

- YYYY: Year
- MM: Month
- DD: Day
- HH: Hour
- MM: Minute
- SS: Second

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster aaa audit Commands

Description Use the `set cluster < name > aaa audit` commands to disable and enable, or configure HTTP(S) authentication auditing.

set cluster aaa audit

Description This command disables or enables HTTP(S) authentication auditing. A license is required for the audit option.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa audit <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa audit level

Description This command sets the level at which authentication messages are written into the audit log. If `all` is selected, all authentication messages are shown. If `failure` is selected, only authentication failures are shown.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> aaa audit level [all | failures]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication Commands

Use the `set cluster <name> aaa authentication` commands to set the HTTP(S) authentication and authorization parameters for a cluster. For additional information about HTTP(S) authentication, see the *Installation and Administration Guide for DXOS*.

The protocol must be set (LDAP and RADIUS), before the `ldap` and `radius` options can be set.

set cluster aaa authentication

Description Enables or disables authentication.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> aaa authentication <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication cache

Description This command disables or enables authentication caching.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> aaa authentication cache <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication cache maxage

Description Sets the maximum number of minutes to store an authentication cache entry (default is 60).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication cache maxage <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap anonymous

Description Enables or disables anonymous access to the LDAP database. Before disabling anonymous access, you must define at least one bind user.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap anonymous <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap base-dn

Description Sets the root Distinguished Name (DN).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap base-dn <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap bind password

Description Sets the bind user password.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap bind password <password>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap bind user-dn

Description Sets the bind user Distinguished Name (DN).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication bind user-dn <user-dn>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap gid

Description Sets the name of the attribute that holds the group information in the LDAP server database.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap gid <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap server <N> ip

Description Sets the IP address of the LDAP server used for the cluster. N can be either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap server <N> ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap server <N> port

Description Sets the port number of the LDAP server used for the cluster. N can be either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap server <N> port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap server type

Description Sets the type of the LDAP server(s) used for the cluster. The available server types are Active Directory Server (ADS), iPlanet Directory Server (IPLANET), or Netscape Directory Server (NDS).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap server type <ADS | IPLANET | NDS>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap ssl

Description Enables or disables LDAP authentication over SSL (default is disabled).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap ssl <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap ssl cacertfile

Description Sets the certificate authority (CA) certfile for SSL.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap ssl cacertfile <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap ssl uri

Description Sets the URI to the domain name specified in the certificate authority (CA) certfile for SSL. The format is "http:// < domain_name > ".

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap ssl uri <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap uid

Description This command is used to set the name of the attribute that holds the user information in the LDAP server database. The username entered in the browser's authentication dialog is assigned to a `uid` attribute. This can be any attribute, for example, a given name, surname, cn, etc. It is best to use uid as it is normally a unique attribute for each person. The authentication will fail if multiple matches are found. The default value is uid.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap uid <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication ldap version

Description This command is used to set the LDAP protocol version. The default is LDAPv3.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication ldap version <2 | 3>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication method www

Description This command is used to set the method of authentication used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication method www`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication password empty_allowed

Description Enables or disables the acceptance of empty (null) passwords (disabled by default). By default, AAA authentication fails if the password has a null value.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication password empty_allowed <disabled* |
enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication password maxage

Description Sets the maximum number of days a password can be used.

Syntax

```
set cluster <name> aaa authentication password maxage <days>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

set cluster aaa authentication password maxlength

Description Sets the maximum number of characters in a password.

Syntax

```
set cluster <name> aaa authentication password maxlength <number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

set cluster aaa authentication protocol

Description This command is used to set the authentication protocol used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication protocol <ldap | radius>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication radius server ip

Description This command is used to set the IP address of the RADIUS server that will be used for the cluster. N can be either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication radius server N ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication radius server port

Description This command is used to set the port number of the RADIUS server that will be used for the cluster. N can be either 1 or 2.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication radius server N port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication radius server key

Description This command is used to set the authentication key of the RADIUS server that will be used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication radius server key <shared-key>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication radius server retries

Description This command is used to set the number of retries of the RADIUS server that will be used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication radius server retries <integer>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication radius server timeout

Description This command is used to set the timeout value of the RADIUS server that will be used for the cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication radius server timeout <integer>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication realm

Description This command is used to set the realm name that is displayed in the login pop-up dialog box.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication realm <string>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication redirect

Description This command disables or enables redirect on a password change flag set. You need to specify a custom page to redirect users to when a password change flag is received.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication redirect <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication redirect host

Description This command is used to set the remote host from where this URL will be retrieved. By default, the file is local, and the host is the IP address of the cluster.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication redirect host <ip address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication redirect protocol

Description This command is used to set the protocol to use when retrieving the password change custom page. The default is http.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication redirect protocol <http | https>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication redirect url

Description This command is used to redirect to a URL when the ldap server or active directory sends a password change flag. The default is "/auth.shtml".

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication redirect url [/auth.shtml | <user provided
url>]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication response text

Description This command is used to set the authentication HTML message used for the cluster.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> aaa authentication response text <string>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication sso cookie name

Description This command is used to optionally specify the name of Single Sign-On (SSO) cookie for the cluster. The default cookie name is DXAUTH.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication sso cookie name <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication sso cookie timeout

Description This command is used to optionally specify the amount of time before the Single Sign-On (SSO) cookie expires for the cluster, requiring users to provide credentials each time they access applications in the specified SSO domain. The timeout value must be between zero and 525600 minutes (24 hours) inclusive. The default cookie timeout is zero, causing the cookie to expire with the browser.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication sso cookie timeout <integer>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication sso

Description This command is used to enable or disable Single Sign-On (SSO) for the cluster, enabling users to access applications in the same domain without repeatedly providing credentials. An SSO domain must be specified before you can enable this function for a cluster. By default, SSO is disabled.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> aaa authentication sso <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster aaa authentication sso domain

Description This command is used to specify the Single Sign-On (SSO) domain for the cluster. An SSO domain must be specified before you can enable this function for a cluster.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> aaa authentication sso <domain-name>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) HTTP(S) Authentication

set cluster apprule Commands

Use the `set cluster < name > apprule` command to bind an OverDrive AppRule ruleset to a specific cluster, and disable or enable ruleset operations on that cluster.

For the `retry_request` action to work correctly with Page Translation Content (PTC), the factory setting `fcl` must be explicitly enabled (it is disabled by default). Contact your administrator or Juniper Technical Support for assistance

set cluster apprule

Description Disables or enables AppRule operations for a specific cluster.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> apprule <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Application Rules

set cluster apprule limit retrypost

Description Sets a value that acts as a “high-water mark” for the number of bytes that will be stored for a POST request to be retried. If the POST data exceeds this value, then the data is released and the retry mechanism is disabled for this request. The original request will proceed.

If a value of zero is specified, then there is no limit imposed on the POST data amount. This is **VERY DANGEROUS** since it allows a single user to issue a single request and use all of the resources on the box. The default value is 32 Bytes. Most POST requests are typically less than 2 KBytes, so there should not be any problems

with the default range limits. An upper limit of 100 MBytes is provided for installations that demand maximum flexibility.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> apprule limit retrypost <int>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Application Rules

set cluster apprule ruleset

Description Sets the filename for the AppRule ruleset for a specific cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> apprule ruleset <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Application Rules

set cluster balance Commands

Description Use the `set cluster < name > balance` commands to set the load balancing policy for a cluster.

The following types of load balancing are available:

- `Fewest Outstanding Requests:` A new incoming connection will be assigned to the cluster with the fewest outstanding connections.
- `Round-Robin:` All the servers in the list are used sequentially for every new TCP session. For example, if there are three servers (S1, S2, and S3), the first request goes to S1, the second request goes to S2, and the third request goes to S3. The list wraps around when it reaches the end.
- `URL Hash`: Used to improve caching efficiency in clusters that use caching. It causes the DX to hash on the URL. If you always direct requests for the same URL to the same cluster, then only that cluster needs to cache objects for that URL instead of having all the clusters cache all objects.
- `Weighted Round-Robin:` The servers are chosen semi-sequentially. A server is chosen based on its weight. The larger the weight, the higher the probability of the server being chosen.

set cluster balance policy

Description This command is used to set the load balancing policy for a cluster. See "Description" above.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> balance policy <fewestoutstandingrequests | roundrobin |
urlhash | weightedroundrobin>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer

set cluster balance policy urlhash <urllen>

Description This command is used to set the length of the URL that will be hashed.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> balance policy urlhash <urllen>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

set cluster cache Commands

Use the `set cluster <name> cache` command to associate or disassociate a cluster with a specific 3G cache, or to disable or enables caching for a cluster.

set cluster cache

Description Associates a cluster with a named 3G cache.

This command does not take effect until after a `write` operation.

Syntax
```
set cluster <name> cache <name>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) 3G Cache

set cluster cache <disabled | enabled>

Description Disables or enables caching for a cluster (disabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> cache <name> <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) 3G Cache

set cluster compression Commands

Use the `set cluster <name> compression` commands to override the global compression settings for a specific cluster. To change the global compression settings, refer to “set server compression Commands” on page 283.

set cluster compression 2k_padding

Description Disables or enables 2 KByte padding for compression to correct a problem with Internet Explorer (IE) 5.x clients when gzip compression is enabled as Accept-encoding (disabled by default). This problem was fixed in IE 6.x. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression 2k_padding <disabled* | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression browser global

Description Resets the cluster’s browser compression settings to the global defaults.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression browser global
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression browser <type>

Description Sets the compression option for a specific browser (default is recommended).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression browser <ie4 | ie50 | ie51 | ie55 | ie6 | ie7 |
ieother | konqueror | ns4 | ns6 | opera | other | safari> <0-3>
```

0 = no, 1 = gzip, 2 = deflate, 3 = recommended

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression cmt

Description Sets the Custom MIME Type to 1, 2, or 3.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression cmt <1 | 2 | 3> <header>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression cmt [disabled | enabled | global]

Description Disables or enables Custom MIME Type compression (disabled by default). Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression cmt <disabled* | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression flushthreshold

Description Flush compression buffers for the first N bytes of response.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression flushthreshold <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression force

Description Forces the use of one or all compression algorithms (default is all). Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression force <0 | 1 | 2 | global>`

0 = all, 1 = gzip, 2 = deflate

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression global

Description Resets all the cluster compression settings to the global defaults.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression browser global`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression http10

Description Disables or enables compression for HTTP/1.0. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression htt10 <disabled | enabled* | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression javascript

Description Disables or enables compression for application/x-javascript. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression javascript <disabled | enabled* | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression msoffice

Description Disables or enables compression for MS Office (i.e., application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/vnd.ms-project, and application/vnd.visio). Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression msoffice <disabled* | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression octetstream

Description Disables or enables compression for application/octet-stream. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression octetstream <disabled* | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression optimization

Description Disables or enables compression for compression optimization. (No slide). Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression optimization <disabled* | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression pdf

Description Disables or enables compression for application/pdf. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression octetstream <disabled | enabled | global*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression policy

Description Disables or enables server compression:

0 = Enable (default)
1 = Disable
global = Return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression policy <0 | 1 | global>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression sharepoint

Description Disables or enables compression for application/x-vermeer-rpc. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression sharepoint <disabled | enabled | global*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression shockwave

Description Compresses application/x-shockwave Flash. Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression shockwave <disabled* | enabled | global>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster compression targetcompression encoding

Description Sets the target compression standards.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression targetcompression encoding <standard* | browser>`

- `standard`: MUX Content-Encoding header is sent. Standard encoding is applicable in either None or Standard modes (default).
- `browser`: Browser Content-Encoding header is sent. Browser encoding is applicable in the modes, None, Standard, Target, and Target_en.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster compression targetcompression mode

Description Sets target compression modes.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> compression targetcompression mode <none* | standard | target | target_en>`

- None: No target compression (default). If this is set, then the “encoding” configuration is not considered.
- Standard: Target compression enabled. Performs standard multiplexing processing. Applicable for both standard and browser encoding configurations.
- Target: Target compression enabled. Any responses from target are not touched. Encoded responses are not cached, but un-encoded responses are cached. PTC is not run. This is only applicable for encoding configurations of the browser.
- Target_en: Target compression enabled. Encoded responses from target are not touched. Un-encoded responses are compressed following the standard multiplexing logic for compression. Encoded responses are not cached, but un-encoded responses are cached. PTC is not run. This is only applicable for encoding browser configurations.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster compression <text_>

Description Disables or enables compression for each type of text (CSS, HTML, and plain text are enabled by default). Use the `global` argument to return the compression value to its global setting.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> compression <text_css | text_html | text_plain |
text_xcomponent | text_xml> <disabled | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set cluster connbind

Description Use the `set cluster <name> connbind` command to disable or enable connection binding.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> connbind <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster convert302protocol

Description Use the `set cluster <name> convert302protocol` command to enable or disable the conversion of HTTP302 responses from HTTP to HTTPS or from HTTPS to HTTP.

Enabling this option will cause the DX to convert the HTTP302 responses from the target server from HTTP to HTTPS or from HTTPS to HTTP. For example, if the HTTP302 responses from the target server are in the HTTP protocol, enabling this

option will cause the DX to convert the HTTP302 responses sent back to the client into HTTPS protocol.

This is useful when SSL acceleration is enabled on the listen side and the target side remains set to clear traffic. When the target server sends an HTTP 302 response, the DX will automatically convert the HTTP302 response back to the client using HTTPS protocols.

The `convert302protocol` does not remove the port number as part of the conversion. For example, a request to: `http://www.myserver.com:80/salesdesk` will be converted to: `https://www.myserver.com:80/salesdesk`. If you need the port number scrubbed, write an AppRule.

Figure 1 shows a simple interaction diagram demonstrating how the `convert302protocol` feature operates. A client is communicating with a DX over a secure (SSL) connection. The DX is communicating with the origin server over a clear channel. The `convert302protocol` feature dynamically rewrites the protocol field in the URL of outbound location headers such that it correctly indicates HTTPS instead of HTTP.

The commands to enable `convert302protocol` are:

```
add cluster <cluster_name>
set cluster listen vip <ip_address>
set cluster listen port <tcp_port>
set cluster listen ssl enabled
set cluster target host <ip:port>
set cluster target host enabled
set cluster convert302 enabled
```

Description Disables the `convert302protocol`.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> convert302protocol <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

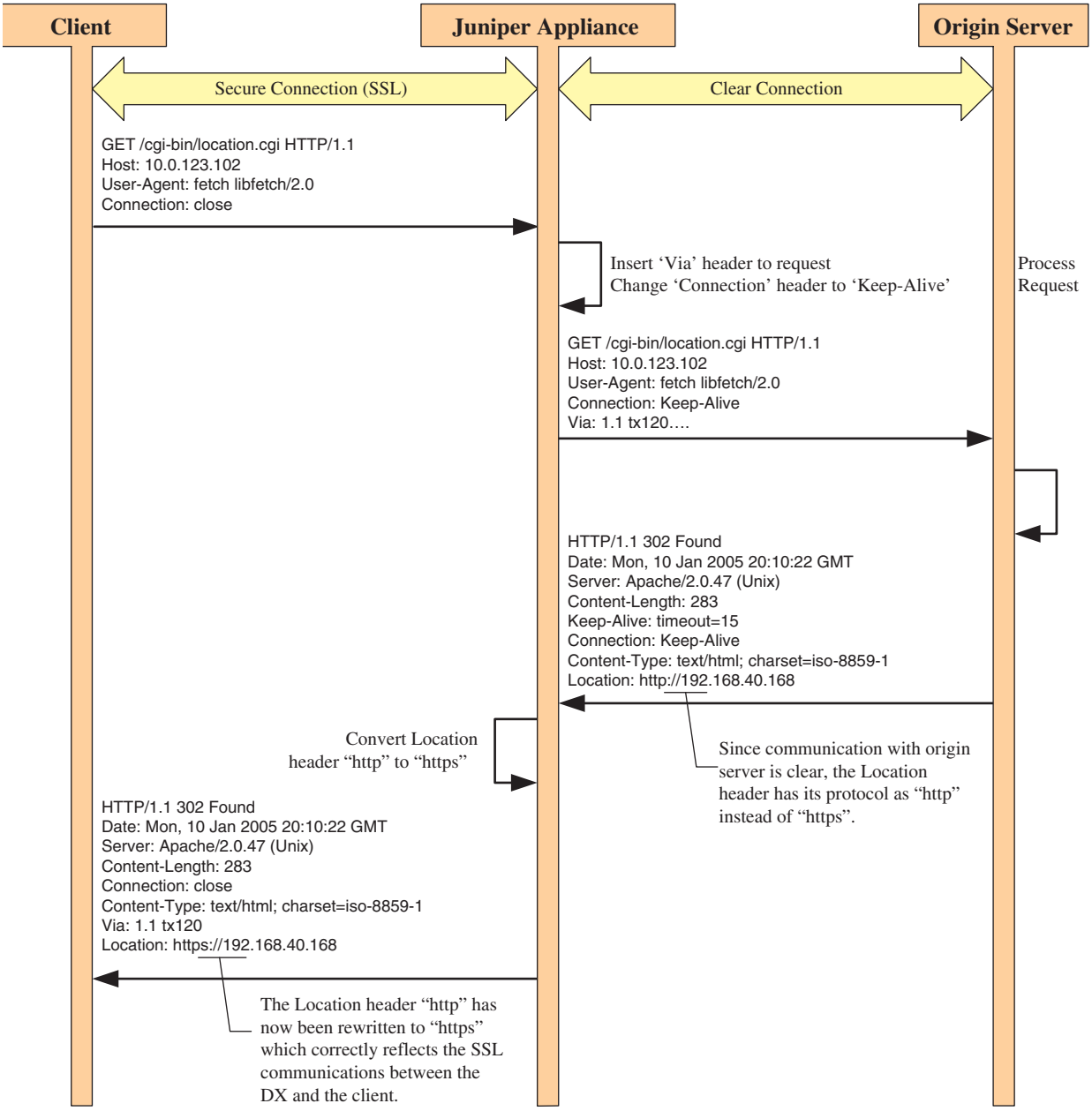

Figure 1: Convert302 Operation

set cluster customiplogheader

Description Use the `set cluster <name> customiplogheader` command to add a logging HTTP header.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> customiplogheader <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster description

Description Use the `set cluster <name> description` command to add a descriptive note to a cluster. This description is limited to 512 characters of free-form text, but cannot include new lines.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> description <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster dsr

Description Use the `set cluster <name> dsr` command to enable or disable Direct Server Return (DSR). This reduces traffic by allowing web servers to send HTTP responses directly back to the requesting client, thus bypassing the load balancer in the response path.

For additional information, see DSR in the *Installation and Administration Guide for DXOS*.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> dsr <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster forwardclientcert headername

Description Use the `set cluster <name> forwardclientdert headername` command to add a header name to the client's certificate when client authentication is performed over SSL. Refer to the *Installation and Administration Guide for DXOS* for more details.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> forwardclientcert headername <header>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster health Commands

Use the `set cluster <name> health` command to set the content health check parameters for target servers.

The DX verifies the health of the target server by sending Layer 4 connection requests and Layer 7 HTTP Get requests to all the target servers in the cluster at a pre-configured interval. The DX assumes all target hosts are down when Layer 7 health checking is turned on, and only logs state transitions. This means that with two servers to be checked when we turn on Layer 7 Health Checking (one down and one up), the server that is up will be logged in the system log as "Server A Passed L7 Health Check" but the server that is down will not be mentioned in the logs until it comes up.

For example:

- Server 0.0.31.20 is Normal: It responds to both a ping and an HTTP request (the machine is up, the web server is up).
- Server 10.0.31.10 is in a Semi-Bad State: It responds to a ping, but not an HTTP request (the machine is up, the web server is down). In this state, when Layer 7 health checking is first enabled, you will never see 10.0.31.10 marked as "bad" by the Layer 7 health check. This is because it was never seen as "up" by the DX, and, therefore, there was never a transition to record.

set cluster health connect interval

Description Number of seconds between Layer 4 connection checks (1 to 3600). Default is 1 second. Note that Layer 4 connection checks can mark a target host as down, but only the Layer 7 health checks and mark a target host as up. Layer 4 connection checks cannot be disabled.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health connect interval <interval>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health connect ssl

Description Enable or disable SSL health check on Layer 4 connections.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health connect ssl <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health connect timeout

Description Maximum number of seconds (1 to 60) that the DX waits to establish a connection during a Layer 4 connection check. Default is 2 seconds.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health connect timeout <1-60>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request <disabled | enabled>

Description Disables or enables content health checks.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request interval

Description Interval for Layer 7 health check requests in seconds (1 to 3600). The default is 15 seconds. The interval should be equal to, or a multiple of, the Layer 4 connection interval (refer to "set cluster health connect interval" on page 176).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request interval <interval>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request resume

Description Number of health checks with good responses before declaring the target server as "operational" (1 to 20). The default is 1.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request resume <resume number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request returncode

Description Expected return code. The default is 200.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health request returncode <return code>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request size

Description Expected size of the response. This is the number of bytes in the body of the response as would be reflected in an HTTP Content-Length header. (The default is zero).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health request size <size of response>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request string

Description Searches for the string in the non-header portion of the HTTP response. This option only applies to the following MIME types:

- text/html
- text/css
- text/plain
- text/xml

The string is case-sensitive, and the maximum length of the string is 64 bytes. When typing the command from the Command Line Interface (CLI), the string must be enclosed in double quotes, if there is white space in the string. The string must **NOT** be enclosed in double quotes when being entered from the WebUI.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health request string <string>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request timeout

Description The timeout value is the maximum time (in seconds) that the DX will wait for the last byte of the HTTP response, measured from the time that the Get request was sent (default is 15 seconds). If this timeout is exceeded, the target will be marked as down with a new status code:

```
RT = Layer 7 Down; Response Timed Out
```

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request timeout <1-60>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request urlpath

Description The URL path that the DX will send to target servers for health checks. The URL path must begin with a "/".

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request urlpath <url path>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health request useragent

Description Sets the user agent for health check requests. The default is Mozilla 4.0, but is compatible with Microsoft Internet Explorer 5.5 and Windows NT.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> health request useragent <default | n>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster health retry

Description Number of consecutive failed health checks required (1 to 20) before the target server is marked as down. The default is 2.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> health retry <retry number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set cluster httpmethod Commands

Use the `set cluster <name> httpmethod` command to disable or enable the Forward Proxy Accelerator.

Set cluster httpmethod connect

Description Disables or enables support for the connect method.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> httpmethod connect <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster httpmethod extended

Description Disables or enables support for the extended methods (i.e., delete and trace options).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> httpmethod extended <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster httpmethod webdav]

Description Disables or enables support for the WebDAV methods.

This command does not take effect until after a write operation.

Syntax

```
set cluster <name> httpmethod webdav <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster listen Commands

Use the set cluster <name> listen command to set properties for cluster listen traffic (between the appliance and the client browser). This establishes a virtual IP address, netmask, port, or SSL configuration for a server's cluster listen traffic.

The Instant Redirect feature (redirect <url>) works only with HTTP clusters, not HTTPS.

The settings made by this command will only take effect after a write operation.

set cluster listen port

Description Sets the cluster listen port (default is 80).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen port <port number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster listen qos

Description Sets the DSCP/ToS values on traffic sent to clients (see "set qos Commands" on page 268).

set cluster listen ssl

Description Use `set cluster < name > listen ssl` command to establish properties for a cluster's SSL listen traffic.

The ephemeral key is a debugging aid for export ciphers. The ephemeral keyfile must be a 512-bit RSA key in OpenSSL PEM (base-64) format and, if encoded, must match the password. The 512-bit RSA key must reside in the file: `/usr/rl/etc/cluster/ephpass.pem.`

The SSL key pass phrase (keypass) is not copied as part of the configuration file on the new partition during an upgrade. You can import the keypass by typing the command:

```
%set cluster <n> listen ssl keypass <key password>
```

Supported cipher suites are shown in "Cipher Suites" on page 477.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl autochain

Description Enables or disables SSL autochaining for cluster listen connections. When enabled, this command also sets the root certificate settings.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl autochain <disabled | enabled | rootcert>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl certfile

Description Specifies the SSL certfile for cluster listen connections.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl certfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl cipherfile

Description Specifies the name of the user-defined file containing a list of cipher suites that conform to the OpenSSL standard.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl cipherfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ciphersuite all

Description Allows all supported SSL cipher suites for cluster listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ciphersuite all`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ciphersuite common

Description Allows only the most commonly used cipher suites from both the strong and export groups.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ciphersuite common`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ciphersuite export

Description Allows only the lower security suites that have been traditionally available for export.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ciphersuite export`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ciphersuite file

Description Allows a user-defined list of SSL cipher suites to be used to configure an SSL cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ciphersuite file`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ciphersuite strong

Description Allows only the highest security cipher suites that have only been traditionally available in the United States.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ciphersuite strong`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth

Description Disables or enables SSL Client Certificate Authentication.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl clientauth <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth authtype

Description Disables or enables client authentication for `cluster <name>`. The default is local and provides local authorization. If none is specified, local and remote authentications are disabled. The option (“`none`”) may be used in situations where a client certificate needs to be forwarded to the target host.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl clientauth authtype <local | none>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth cacertfile

Description Sets the advertised Certificate Authority (CA) file as a `<filename>` for the cluster. The `<filename>` must contain a list of one or more valid CA certificates that are self-signed or signed by:

- A well-known trusted CA
- A CA listed in the trusted CA certificate file

All certificate entries in this file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen ssl clientauth cacertfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth cacrlfile

Description Sets the CA Certificate Revocation List (CRL) as a `<filename>` for the cluster. The `<filename>` must be a list of one or more valid CRLs containing certificates signed by one of the CA's listed in the trusted CA certificate file. All CRL entries not corresponding to an entry in the trusted CA certificate file are ignored.

All CRLs listed in the file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen ssl clientauth cacrlfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth catrustfile

Description Sets the CA Trusted Certificate file to `< filename >` for the cluster. The `< filename >` must be a file containing a valid list of one or more root- or intermediate-CA certificates; each certificate is encoded in base64 format.

If the certificate is an intermediate certificate, its root CA certificate must also be present in either a `catrustfile` or the `cacertfile`.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl clientauth catrustfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth forwardclientcert

Description Disables or enables forwarding of client certificates to the target host as an HTTP header (default is disabled).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl clientauth forwardclientcert <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl clientauth forwardclientcert format

Description Sets the format of the certificate to be forwarded as an HTTP header. (The default is X509 certificate in DER format base-64 encoded (DERBase64).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl clientauth forwardclientcert format DERBase64|PEM`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl

Description Disables or enables SSL for cluster listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ephkeyfile

Description Specifies the SSL ephemeral keyfile.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ephkeyfile <ephkeyfile>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl ephkeypass

Description Specifies the ephemeral key pass phrase.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> listen ssl ephkeypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl keyfile

Description Specifies the SSL keyfile for cluster listen traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen ssl keyfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl keypass

Description Specifies the SSL key pass phrase for cluster listen traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen ssl keypass
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen ssl protocol

Description Specifies the SSL protocol type for cluster listen traffic:

- sslv2: SSL Version 2 only
- sslv23: SSL Version 2; SSL Version 3: TLS Version 1
- sslv3: SSL Version 3 only
- tlsv11: TLS Version 1 only

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen ssl protocol <sslv2 | sslv23 | sslv3 | tlsv1>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster listen targetdown

Description Sets the behavior when all targets are down.

- `blackhole`: Refers to the current behavior of dropping all packets sent to the cluster that has all of its target hosts down.
- `finclient:` Refers to the historical behavior of allowing the client to connect and then subsequently closing down the connection with a FIN.
- `redirect <url>`: Redirects clients with an HTTP 302 reply to the new location specified in `<url>`.

The URL is specified as follows:

```
http://<server>[:port][/path/resource]
```

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen targetdown <blackhole | finclient | redirect> <url>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster listen vip

Description Sets the cluster listen Virtual IP address.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> listen vip <ip>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster name

Description Changes the name of a cluster.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> name <newname>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster owa

Description Use the `set cluster owa` command to disable or enable support for Outlook Web Access (OWA).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> owa <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sacompat Commands

Use the `set cluster <name> sacompat` commands to enable or disable DX compatibility with the Juniper Secure Access SSL VPN (SA) solution, and to define any required URLs.

set cluster sacompat

Description Enables or disables the ability of a specified DX cluster to provide Juniper SA solution Network Connect Protocol (NCP) compatibility. The default is disabled.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> sacompat <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set cluster sacompat advanced url

Description Specifies one of three URLs used for SA compatibility. If a URL is configured, the DX determines if the specified cluster should drop into forwarder mode. The first URL defaults to `/dana/j`.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sacompat advanced url <1 | 2 | 3>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set cluster sacompat advanced defaults

Description Returns the three URLs settings used for SA compatibility to their default value. The first URL defaults to `/dana/j`. The second and third URL default to an empty string.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sacompat advanced defaults`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set cluster stats history

Description Disables or enables the collection of statistics history.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> stats history <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky Commands

Use the `set cluster <name> sticky` commands to set client to target sever bindings.

set cluster sticky clientip leader

Description Specifies whether a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group (the default is none). This creates a sticky group so that client applications with multiple protocol flows (such as TCP and UDP) can be load balanced to the same target host. The sticky method must be clientip (see "set cluster sticky method" on page 195).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> sticky clientip leader <none | <<cluster | forwarder | slb group> <name>>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky clientip timeout

Description Sets the number of minutes (1 to 43200) a client IP is bound to a target host. The default value is 120.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> sticky clientip timeout
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky cookie expire

Description Sets the number of minutes a cookie is valid. The range is 1 minute to 3,000,000 minutes (5.71 years). Setting the value to zero means the cookies never expire.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> sticky cookie expire
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky cookie mask iponly

Description Uses only the IP address to identify a target server.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sticky cookie mask iponly`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky cookie mask ipport

Description Uses both the IP address and the port to identify a target server.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sticky cookie mask ipport`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky cookie passheader

Description Instructs the DX to remove the sticky cookie from the request headers. If enabled (the default), the cookie is passed through. If disabled, the cookie is stripped.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sticky cookie passheader <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster sticky failover

Description Enables or disables sticky failover for the specified cluster. When Unified Failover is also enabled, the standby DX takes on communications for the specified cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sticky failover <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) Global Configuration

set cluster sticky method

Description Specifies whether cookies or client IP addresses are used to bind clients to a target host (the default is none).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> sticky method <clientip | cookie | none>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster target Commands

Use the `set cluster <name> target` command to set a target name or target host, tune a target host, and/or to disable or enable the target host.

set cluster target host <all | ip:port>

Description Adds a target host to cluster; "all" can be specified instead of ip and/or port.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target host <all | <ip:port>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

set cluster target host <ip:port> <disabled | enabled>

Description Disables or enables the cluster target host.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target host <all | <ip:port> <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set cluster target host <all | ip:port> <hardpaused | softpaused | unpaused>

Description Pauses or unpauses traffic to one or all target hosts (default is unpaused). A "hard" pause terminates all existing traffic, while a "soft" pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set cluster <name> target host <all | <ip:port> <hardpaused | softpaused |
unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Global Configuration

set cluster target localip

Description Sets the local IP to be used for communication with all the target hosts in this cluster.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target localip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster target name <dns name>

Description Sets the cluster target name.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target name <dns name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster target qos

Description Sets the DSCP/ToS values on traffic sent to host servers (see “set qos Commands” on page 268).

set cluster target ssl

Description Use the `set cluster < name > target ssl` command to establish SSL properties of target servers.

Supported cipher suites are shown in "Cipher Suites".

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl autochain

Description Enables or disables SSL autochaining for cluster target connections. When enabled, this command also sets the root certificate settings.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl autochain <disabled | enabled | rootcert>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl certfile

Description Specifies the SSL certfile for cluster target connection.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl certfile <file>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl cipherfile

Description Specifies the name of the user-defined file containing a list of cipher suites that conform to the OpenSSL standard.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl cipherfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl ciphersuite all

Description Allows all supported SSL cipher suites for cluster target traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl ciphersuite all
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl ciphersuite common

Description Allows only the fastest cipher suites from both the strong and export groups.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl ciphersuite common
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl ciphersuite export

Description Allows only the lower-security cipher suites that are suitable for export.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target ssl ciphersuite export`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl ciphersuite file

Description Allows a user-defined list of SSL cipher suites to be used to configure an SSL target.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target ssl ciphersuite file`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl ciphersuite strong

Description Allows only the highest security cipher suites that are suitable for use in the United States.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target ssl ciphersuite strong`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl

Description Disables or enables SSL for cluster target traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl keyfile

Description Specifies the SSL keyfile for cluster target connections.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl keyfile <file>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl keypass

Description Specifies the SSL key pass phrase for cluster target connections.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> target ssl keypass
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl protocol

Description Specifies the SSL protocol type for cluster target traffic:

- sslv2: SSL Version 2 only
- sslv23: SSL Version 2; SSL Version 3; TLS Version 1
- sslv3: SSL Version 3 only
- tlsv1: TLS Version 1 only

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target ssl protocol [sslv2 | sslv23 | sslv3 | tlsv1]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target ssl timeout

Description Timeout in number of minutes (default is 1440 minutes).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> target ssl timeout <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set cluster target tune

Description Use the `set cluster < name > target tune` command to start the target-tuning tool. The purpose of the target-tuning tool is to enable you to easily set up the interaction within the target hosts, and to properly set up the cluster/system behavior for a custom environment. The target-tuning tool is a single CLI command that sets a number of configuration variables using a question and answer format.

The set cluster <name> target tune command prompts you for the options shown in Table 3, Table 4, and Table 5.

Table 3: Target Application Tune Options

Options	Action
Other*	Selecting this option resets all the setting changes made by the other selections for this item to their "default" value. The settings that it affects are: ■ Disable Extended HTTP Methods ■ Disable WebDAV HTTP Methods ■ Disable Connection Binding ■ Disable compression of unauthorized responses ■ Disable compression of MIME type "text/xml" ■ Disable compression of MIME type "text/x-component" ■ Enable compression of MIME type "text/plain" ■ Set Standing Connection (sc) to six ■ Disable compression of MS Office documents ■ Reset the custom MIME type for "application/pdf" ■ Disable use of custom MIME types ■ Enable the use of the HTTP Vary header
PeopleSoft	This option disables compression of MIME type "text/plain" serverwide
Domino 5	This option makes the following settings: ■ Enable Connection Binding for this cluster ■ Set Standing Connection (sc) to 0 (zero) serverwide
Domino 6	This option sets Standing Connection (sc) to two serverwide
JDE OneWorld	This option makes the following settings: ■ Enable compression of MS Office documents serverwide ■ Turn off the use of 2k (default value) ■ Set a custom MIME type for "application/pdf" serverwide ■ Enable use of custom MIME types serverwide ■ Disable the use of the HTTP Vary header serverwide
OWA	This option makes the following settings: ■ Enable Extended HTTP Methods for this cluster ■ Enable WebDAV HTTP Methods for this cluster ■ Enable Connection Binding ■ Enable compression of unauthorized responses for this cluster ■ Enable compression of MIME type "text/xml" serverwide ■ Enable compression of MIME type "text/x-component" serverwide
Fwd Proxy	This option sets the type of forward proxy (Apache, IIS4, or Other)

The tuning options for the Target Web Server type are:

Table 4: Target Web Server Tuning Options

Options	Action
Other*	Selecting this option disables protected TelnetClient tc3 support serverwide.
Apache	Selecting this option enables protected TelnetClient tc3 support serverwide.
IIS4	Selecting this option enables protected Internet Information Server support serverwide.

The tuning options for the NTLM Authentication are:

Table 5: NTLM Authentication Tuning Options

Options	Action
No*	Selecting this option disables connection binding for this cluster.
Yes	Selecting this option enables connection binding for this cluster.

The settings made by this command will only take effect after a write operation.

Syntax `set cluster <name> target tune`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Example An example of a typical tuning tool session is shown below. The default answer for each of the questions is marked with an asterisk (*):

```
% set cluster 1 target tune

This will help optimize the communication with the Target Hosts
within this cluster. It will help ensure that functionality is
maintained while providing the most possible benefit.

Please answer the following questions. Enter Control-C at any
time to exit without modification.

1) Please select the Target Application
1) Other (*)
2) PeopleSoft
3) Domino5
4) Domino6
5) JDE
6) OWA

Enter Selection: 1

2) Please select the Target Web Server Type
1) Other (*)
2) Apache
3) IIS4
Enter Selection: 1

3) Is NTLM Authentication used?
N) No (*)
Y) Yes

Enter Selection: n

You have selected:
Target Application: Other
Target Web Server: Other
NTLM Authentication: No
```

```
Continue using these selections?
N) No, Start Over (*)
Y) Yes, Use these values

Enter Selection: y

Tuning based on your selections ...

Done.
(*) dx5
```

set cluster transparency

Description

Use the `set cluster < name > transparency` command to enable or disable IP transparency. DXs operate in a secure reverse-proxy mode. In this mode, all incoming client requests are terminated at the DX and multiplexed to a pool of predefined target hosts that serve the content. When the DX provides connection multiplexing, the Source IP (SIP) is replaced by the IP of the DX before the request is forwarded to the target host. This is required to provide the connection multiplexing capability in the DX. However, this may create unintended side effects:

- The target host logs do not have the client's IP address any longer.
- Since to the target host, all requests look to originate from a single IP, it may perceive it as an attack and close connections.

The `set cluster <name> transparency` command allows you to enable or disable client IP transparency capability for a cluster configuration. Enabling transparency allows the target hosts to see the source IP address of the originating connection. For more information, see Client IP Transparency in the "Integrating the DX Introduction" chapter of the *Installation and Administration Guide for DXOS*.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> transparency <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set cluster weblog Commands

Use the `set cluster <name> weblog` commands to configure Web log settings. The DX can be configured to transmit the logs to the Syslog server in one of two ways. The default configuration is Immediate mode, where the DX immediately writes a User Datagram Protocol (UDP) packet containing a web log to the configured Syslog server for each client request. Immediate mode can create a significant amount of extra network activity and does not allow the ability to save logs.

The alternative is Web Log Batch mode. In Web Log Batch mode, web logs are saved on the DX and then copied off in bulk format.

The user can select the log format from one of these five options:

- `common`: This is the Apache Common Logging Format (CLF). The information included in the log is:

  remotehost remotelogname authuser [date] “request” status bytes

- `combined`: This is a modification of CLF (common) format and adds the values of the Referer and User-Agent HTTP headers in quotes:

  remotehost remotelogname authuser [date] “request” status bytes “Referer” “User-Agent”

- `common_cn`: This is a modification of CLF (common) format with the cluster name prepended to the CLF format:

  clustername remotehost remotelogname authuser [date] “request” status bytes

- `combined_cn`: This is a modification of the combined format with the cluster name prepended to the combined format:

  clustername remotehost remotelogname authuser [date] “request” status bytes “Referer” “User-Agent”

- `perf1`: This is a proprietary format that lets you easily monitor the performance of the DX compression and cache. The information included in the log is:

  remotehost [date] method url version status request-bytes precomp-bytes postcomp-bytes cachehit

- `perf2`: This is a proprietary format that lets you troubleshoot performance problems. The information included in the log is: `ip_por`t from result transactionID T1 T2 T3 T4 Granularity.

Information fields included in the logs are shown in Table 6.

Table 6: Web Log Field Definitions

Field	Definition
remotehost	Remotehost name (or IP address if the DNS hostname is not available, or if the DNS Lookup is off).
remotelogname	Remote logname of the user.
authuser	Username with which the user authenticated himself.
[date]	Date and time of the request inside brackets ([ ]).
“request”	Request line exactly as it came from the client inside quotes (“ “).
status	HTTP status code returned to the client.
bytes	Content-length of the document transferred for response.
“referer”	Value of the Referer header inside quotes (“ “).
“user-agent”	Value of the User-Agent header inside quotes (“ “).

Table 6: Web Log Field Definitions (continued)

Field	Definition
clustername	Name of the cluster that received the request.
method	Request method.
url	Request URL.
request-bytes	Length of request content-body. This is applicable for POST, PUT, and certain WebDAV requests.
precomp-bytes	Content-length of the response document before compression.
postcomp-bytes	Content-length of the response document after compression.
cachehit	Number of Juniper cache hits or cache misses.

set cluster weblog

Description Disables or enables cluster logging.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch compression

Description Disables or enables the use of GZIP compression for Syslog entries sent in batch mode (enabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog batch compression <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch copy copynow

Description Forces an immediate copy of the Web Logs to the configured Syslog server.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog batch copy copynow
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch copy interval

Description Sets a periodic interval for the Web Logs to be sent to the configured Syslog server.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch copy interval <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch copy size

Description Sets the size of the compressed file to copy (the size of the two data buffers). The range is 1 to 50 MByte (default is 10 MBytes).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch copy size<val>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch copy time

Description Sets the times for the Web Log to be transmitted to the configured Syslog server. The format of [time] is HH:MM. Up to three times can be configured for each day.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch copy time <1|2|3> <time>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch failure retryinterval

Description Sets the retry interval (in seconds) in case of copy failure. The range is 30 to 200 seconds (default is 60 seconds).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch failure retryinterval <val>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch host

Description Sets the host where the Web Log will be copied.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch host <server>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch scp connecttest

Description This command is used to test the connection (copies a one byte test file).

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch scp connecttest`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch scp directory

Description Sets the remote scp target directory.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch scp directory <directory>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch scp keyfile

Description Sets the (non-password protected) private key. The private key must then be captured using the `capture` command. For additional information, see “capture Commands” on page 24.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch scp keyfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog batch scp username

Description Sets the remote scp username.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog batch scp username <user>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog delimiter

Description Sets the delimiter in the Web Log to be either a comma or a space.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog delimiter <comma | space>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog destination

Description Specifies whether Web Log entries are sent to the Syslog server immediately (syslog) or in a batch (batch). The default is syslog.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog destination <batch | syslog*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog format

Description Sets the format for the Web Log.

This command does not take effect until after a `write` operation.

Syntax

```
set cluster <name> weblog format <combined | combined_cn | common | common_cn |
perf1 | perf2>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog syslog host

Description Sets the cluster log host address.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog syslog host <ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set cluster weblog syslog port

Description Sets the port where the Web Log will be sent. The default port is 514.

This command does not take effect until after a `write` operation.

Syntax `set cluster <name> weblog syslog port <port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Historical Rates and Statistics

set dns Commands

Use these commands to set the DNS domain name and DNS servers.

set dns domain

Description Sets the name service domain.

This command does not take effect until after a `write` operation.

Syntax `set dns domain <dns name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set dns server

Description Sets the name service. N = 1, 2, or 3.

This command does not take effect until after a `write` operation.

Syntax `set dns server <N> <ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ether Commands

Description Use the set ether <n> commands to set the IP address, media, MTU, and netmask (where n is 0 or 1).

The administrative interface can be all interfaces or those specified by the `set admin interface` command. The setting for media must exactly match the switch to which the DX is attached. If the switch is managed and has explicit settings, choose the exact speed and setting. If the switch is un-managed, choose auto-negotiate. The Maximum Transmission Unit (MTU) should be set to 1500 for Ethernet.

DO NOT change this value unless your switch and network are configured to work with a different MTU.

set ether ip

Description Sets the ether n IP address.

This command does not take effect until after a `write` operation.

Syntax `set ether <n> ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ether <n> media

Description Sets media parameters. Supported media options are:

- 10baseT/UTP
- 10baseT/UTP full-duplex
- 100baseTX
- 100baseTX full-duplex
- 1000baseTX (DX 36xx models only)
- 1000baseTX full-duplex (DX 36xx models only)
- autoselect

This command does not take effect until after a `write` operation.

Syntax `set ether <n> media <media description or #>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ether mtu

Description Sets the interface Maximum Transmission Unit (MTU).

This command does not take effect until after a `write` operation.

Syntax `set ether <n> mtu <mtu #>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ether netmask

Description Sets the netmask.

This command does not take effect until after a `write` operation.

Syntax `set ether <n> netmask <ip mask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set failover Commands

Use the `set failover` commands to configure Unified Failover. Unified Failover lets you specify a single failover configuration that applies to each of the following services:

- ActiveN
- Forward Proxy Accelerator (also called the DX server)
- Server Load Balancing (SLB
- Global Server Load Balancing (GSLB))

To use Unified Failover, you must disable the individual failover configurations for each service (the two failover methods are mutually exclusive).

When Unified Failover is activated, failover is enabled for each active service that supports it (currently the DX server, SLB, GSLB, and ActiveN). The Appliance Discovery and Failover Protocol (ADFP) is used to dynamically discover all DX peers in the same network that are enabled for Unified Failover. Peers on remote networks, such as remote GSLB nodes, can be defined manually as static peers.

A master node can be designated manually or negotiated among the peers. The master node aliases the VIPs, floating VIPs, and VMACs for the other peers, which remain in standby mode,. Whenever the master fails over, two SNMP traps are generated (failoverStateMaster by the new master, and failoverStateStandby by the previous master).

Most services run only on the master. However, if you activate both the DX server and ActiveN to do load balancing across multiple nodes, the server runs on each node, and Unified Failover monitors only ActiveN.

After Unified Failover is disabled, each service can be enabled or disabled manually, and rebooting the DX will start all enabled services.

set failover

Description Enables or disables Unified Failover (disabled by default). Enabling failover initiates failover processing. Disabling failover on a DX stops the failover processing (if the DX is the master, a standby peer, if any, becomes the new master).

This command does not take effect until after a `write` operation.

Syntax

```
set failover <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover advanced

Description Changes the defaults for the following settings:

- pollinterval. Number of seconds between polls used to verify the availability of the other peers (default is five seconds).
- missedcount. Number of consecutive polls with no response that indicate a peer is unavailable (default is three).
- serviceinterval. Number of seconds that a service can be down before a failover occurs (default is eight seconds).

This command does not take effect until after a `write` operation.

Syntax

```
set failover advanced <missedcount <N> |pollinterval <seconds> | serviceinterval
<seconds>>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover discovery interface

Description Sets the interface used to discover the other peers enabled for Unified Failover (default is ether0). The IP address of the discovery interface is used as the source IP address on all outgoing discovery protocol traffic. If the discovery interface is changed, the source IP is changed, and the peers assume that the new IP address is for a different interface on the same DX.

This command does not take effect until after a `write` operation.

Syntax

```
set failover discovery interface ether <N>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover discovery port

Description Sets the port number used to discover peers enabled for Unified Failover (default is 9500). The ADFP Discovery packets are sent to this port.

This command does not take effect until after a `write` operation.

Syntax

```
set failover discovery port <N>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover forcemaster

Description Enables or disables a device as the master (disabled by default). You can force a standby node to become the master at any time. If forcemaster is set on multiple peers, the peer with the lowest node ID becomes the master.

This command does not take effect until after a `write` operation.

Syntax

```
set failover forcemaster <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover linkfail

Description Enables or disables failover for one or all links when a link fails (enabled for all links by default). When the master detects that a monitored link is down, the master fails over to ensure that a second master is not activated when the standby peers detect that the master is unavailable. When a failover starts, a warning is shown if any links are down.

This command does not take effect until after a `write` operation.

Syntax

```
set failover linkfail ether <all | N> <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover listen port

Description Sets the port number used to listen for ADFP Active and Standby packets (default is port 9500).

This command does not take effect until after a `write` operation.

Syntax `set failover listen port <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover nodeid

Description Sets the node ID for the device. Enter auto to generate an ID from the IP address (default is auto). Unless forcemaster is set on one of the peers, the peer with the lowest node ID becomes the master.

This command does not take effect until after a `write` operation.

Syntax `set failover nodeid <N> | “auto”`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover peer

Description Enables or disables failover communication with one or all static peers (enabled by default). To add a remote peer, see “add failover peer” on page 17.

This command does not take effect until after a `write` operation.

Syntax `set failover peer <ip | all> <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover peer listen port

Description Sets the port number used by one or all remote static peers to listen for ADFP Active and Standby packets (default is port 9500). To add a remote peer, see “add failover peer” on page 17.

This command does not take effect until after a `write` operation.

Syntax
```
set failover peer <ip | all> listen port <N>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover stateful

Description Enables or disables sticky failover on the DX. Unified Failover must be enabled (see set failover on page 215) for this command to have an effect. Sticky failover is disabled by default.

This command does not take effect until after a `write` operation.

Syntax
```
set failover stateful <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) Unified Failover

set failover stateful syncinterval

Description Specifies the interval at which state information on the standby DX is synchronized with that on the master DX. Valid values range from one second to 3600 seconds. The default value is one second.

This command does not take effect until after a `write` operation.

Syntax
```
set failover stateful syncinterval <interval>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) Unified Failover

set failover vmac ether

Description Enables or disables the use of a VMAC address on one or all interfaces (enabled by default). N is the interface number, such as 0 or 1.

This command does not take effect until after a `write` operation.

Syntax `set failover vmac ether <N | all> <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set failover vmac ether id

Description Sets a VMAC ID (1 to 254) for one or all interfaces that determines the VMAC address (default is "1" for ether1 and "2" for ether2). N is the interface number, such as 0 or 1.

This command does not take effect until after a `write` operation.

Syntax `set failover vmac ether <N | all> id <1-254>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Unified Failover

set forwarder Commands

A forwarder is used to forward non-HTTP TCP traffic (such as SMTP traffic).

- Use the `set forwarder <name> listen` command to set the address or port for forwarder listening.
- Use the `set forwarder <name> name` command to rename a forwarder.
- Use the `set forwarder <name> target` command to establish a target host, and/or enable or disable that host.
- Use the `set forwarder <name> weblog` command to set the host or logging for a forwarder.

The description is limited to 512 characters of free-form text, but cannot include new lines. This allows administrators to fully describe forwarder usage, contact information, warnings, or any other pertinent information they deem necessary.

Load balancing options are:

- Round-Robin: All the servers in the list are used sequentially for every new TCP session. For example, if there are three servers (S1, S2, and S3), the first request goes to S1, the second request goes to S2, and the third request goes to S3. The list wraps around when it reaches the end.
- Weighted Round-Robin: The servers are chosen semi-sequentially. A server is chosen based on its weight. The larger the weight, the higher the probability of the server being chosen.

set forwarder balance policy

Description This command is used to set the load balancing policy for a cluster (default is roundrobin). For additional information, see the "Notes" for command "set forwarder Commands" on page 220.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> balance policy <roundrobin | weightedroundrobin>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder description

Description Adds a description to the forwarder `<name>`.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> description <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder dsr

Description Disables or enables Direct Server Return (DSR) for the named forwarder.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> dsr <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder health connect interval

Description Number of seconds between Layer 4 connection checks (1 to 3600). Default is one second. Note that Layer 4 connection checks can mark a target host as down, but only the Layer 7 health checks can mark a target host as up. Layer 4 connection checks cannot be disabled.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> health connect interval <interval>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set forwarder health connect timeout

Description Maximum number of seconds (1 to 60) that the DX waits to establish a connection during a Layer 4 connection check. Default is two seconds.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> health connect timeout <1-60>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set forwarder health retry

Description Number of consecutive failed health checks required (1 to 20) before the target server is marked as down. The default is 2.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> health retry <1-20>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Health Checking

set forwarder listen port

Description Sets the forwarder's listen port (the default is 80).

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder listen qos

Description Sets the DSCP/ToS values on traffic sent to clients (see "set qos Commands" on page 268).

set forwarder listen ssl certfile

Description Specifies the SSL certfile for forwarder listen connections.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl certfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl cipherfile

Description Specifies the name of the user-defined file containing a list of cipher suites that conform to the OpenSSL standard.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl cipherfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ciphersuite all

Description Allows all supported SSL cipher suites for forwarder listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ciphersuite all`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ciphersuite common

Description Allows only the most commonly used cipher suites from both the strong and export groups.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ciphersuite common`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ciphersuite export

Description Allows only the lower-security cipher suites that have been traditionally available for export.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ciphersuite export`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ciphersuite file

Description Allows a user-defined list of SSL cipher suites to be used to configure an SSL forwarder.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ciphersuite file`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ciphersuite strong

Description Allows only the highest-security cipher suites that have only been traditionally available in the United States.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ciphersuite strong`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl clientauth

Description Disables or enables SSL client authentication for the listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl clientauth <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl clientauth authtype

Description Disables or enables client authentication for forwarder `< name >`. The default is local and provides local authorization. If none is specified, the local and remote authentication are disabled. The option ("none") may be used in situations where a client certificate needs to be forwarded to the target host.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> listen ssl clientauth authtype <local | none>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl clientauth cacertfile

Description Sets the advertised Certificate Authority (CA) file as a `<filename>` for the forwarder. The `<filename>` must contain a list of one or more valid CA certificates that are self-signed or signed by:

- A well-known trusted CA
- A CA listed in the trusted CA certificate file

All certificate entries in this file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> listen ssl clientauth cacertfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl clientauth cacrlfile

Description Sets the CA Certificate Revocation List (CRL) as a `< filename >` for the forwarder. The `< filename >` must be a list of one or more valid CRLs containing certificates signed by one of the CA's listed in the trusted CA certificate file. All CRL entries not corresponding to an entry in the trusted CA certificate file are ignored.

All CRLs listed in the file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl clientauth cacrlfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl clientauth catrustfile

Description Sets the CA Trusted Certificate file to a `< filename >` for the forwarder. The `< filename >` must be a file containing a valid list of one or more root- or intermediate-CA certificates; each certificate is encoded in base64 format.

If the certificate is an intermediate certificate, its root CA certificate must also be present in either a catrustfile or the cacertfile.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl clientauth catrustfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl

Description Disables or enables SSL for forwarder listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl autochain

Description Enables or disables SSL autochaining for forwarder listen connections. When enabled, this command also sets the root certificate settings.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> listen ssl autochain <disabled | enabled | rootcert>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ephkeyfile

Description Specifies the SSL ephemeral keyfile. The ephemeral key is a debugging aid for export ciphers. The ephemeral keyfile must be a 512-bit RSA key in OpenSSL PEM (base-64) format and, if encoded, must match the password. The 512-bit RSA key must reside in the file: `/usr/rl/etc/forwarder/ephpass.pem`.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> listen ssl ephkeyfile <ephkeyfile>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl ephkeypass

Description Specifies the ephemeral key pass phrase. The SSL key pass phrase (keypass) is not copied as part of the configuration file on the new partition during an upgrade. You can import the keypass by typing the command:

```
%set forwarder <n> listen ssl ephkeypass <key password>
```

Supported cipher suites are shown in “Cipher Suites” on page 477

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl ephkeypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl keyfile

Description Specifies the SSL keyfile for forwarder listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl keyfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl keypass

Description Specifies the SSL keypass phrase for forwarder listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen ssl protocol

Description Specifies the SSL protocol type for forwarder listen traffic:

- sslv2: SSL Version 2 only
- sslv23: SSL Version 2; SSL Version 3: TLS Version 1
- sslv3: SSL Version 3 only
- tlsv1: TLS Version 1 only

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen ssl protocol [sslv2 | sslv23 | sslv3 | tlsv1]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder listen vip

Description Sets the forwarder's Virtual IP address.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> listen vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder name

Description Renames a forwarder from `<name>` to `<new name>`.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> name <new name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder sticky clientip leader

Description Specifies whether a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group (the default is none). This creates a sticky group so that client applications with multiple protocol flows (such as TCP and UDP) can be load balanced to the same target host. The sticky method must be clientip (see "set forwarder sticky method" on page 232).

This command does not take effect until after a `write` operation.

Syntax
```
set forwarder <name> sticky clientip leader <none | <<cluster | forwarder | slb group> <name>>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder sticky clientip timeout

Description Sets the maximum number of minutes (1 to 43200) between consecutive client requests that are bound to the same target host (default is 120).

This command does not take effect until after a `write` operation.

Syntax
```
set forwarder <name> sticky clientip timeout
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder sticky failover

Description Enables or disables sticky failover for the specified forwarder. When Unified Failover is also enabled, the standby DX takes on communications for the specified forwarder.

This command does not take effect until after a `write` operation.

Syntax
```
set forwarder <name> sticky failover <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X		X			

Mode(s) Global Configuration

set forwarder sticky method

Description Specifies whether consecutive requests from the same client IP address within the specified timeout can be bound to the same target host (default is none).

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> sticky method <clientip | none>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder target host

Description Adds the IP address and the port for the forwarder target.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target host <ip:port>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

set forwarder target host <ip:port> <hardpaused | softpaused | unpaused>

Description Pauses or unpauses traffic to a target host (default is unpaused). A “hard” pause terminates all existing traffic, while a “soft” pause does not affect existing traffic.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target host <ip:port> <hardpaused | softpaused | unpaused>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

set forwarder target host <ip:port> maxconnections

Description Sets the maximum number of concurrent connections for a target host. A zero indicates no limit (the default).

Syntax This command takes place immediately; no `write` command is needed. Enter a `write` command to retain the change after the next reboot.

```
set forwarder <name> target host <ip:port> maxconnections <N>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder target host <ip:port> weight

Description Sets the weight of a target host (default is 1). If weighted round-robin is enabled, the larger the weight, the higher the probability of the target host being used.

Syntax This command takes place immediately; no `write` command is needed. Enter a `write` command to retain the change after the next reboot.

```
set forwarder <name> target host <ip:port> weight <N>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder target localip

Description Sets the local IP address to be used for communication with all the target hosts in this forwarder.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target localip <ip>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set forwarder target qos

Description Sets the DSCP/ToS values on traffic sent to target hosts (see “set qos Commands” on page 268).

set forwarder target ssl

Description Disables or enables SSL for forwarder target traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl autochain

Description Enables or disables SSL autochaining for forwarder target connections. When enabled, this command also sets the root certificate settings.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl autochain <disabled | enabled | rootcert>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl certfile

Description Specifies the SSL certfile for forwarder target connections.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl certfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl cipherfile

Description Specifies the name of the user-defined file containing a list of cipher suites that conform to the OpenSSL standard.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl cipherfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl ciphersuite all

Description Allows all supported SSL cipher suites for forwarder target traffic.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl ciphersuite all
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl ciphersuite common

Description Allows only the fastest cipher suites from both the strong and export groups.

This command does not take effect until after a `write` operation.

Syntax

```
set forwarder <name> target ssl ciphersuite common
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl ciphersuite export

Description Allows only the lower-security cipher suites that are suitable for export.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl ciphersuite export`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl ciphersuite file

Description Allows a user-defined list of SSL cipher suites to be used to configure an SSL target.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl ciphersuite file`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl ciphersuite strong

Description Allows only the highest security cipher suites that are suitable for use in the United States.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl ciphersuite strong`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl keyfile

Description Specifies the SSL keyfile for forwarder target connections.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl keyfile <file>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl keypass

Description Specifies the SSL key pass phrase for forwarder target connections.

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl protocol

Description Specifies the SSL protocol type for forwarder target traffic:

- sslv2: SSL Version 2 only
- sslv23: SSL Version 2; SSL Version 3; TLS Version 1
- sslv3: SSL Version 3 only
- tlsv1: TLS Version 1 only

This command does not take effect until after a `write` operation.

Syntax `set forwarder <name> target ssl <sslv2 | sslv23 | sslv3 | tlsv1>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set forwarder target ssl timeout

Description Sets the SSL session timeout (in minutes) for the forwarder's target traffic.

This command does not take effect until after a `write` operation.

Syntax
```
set forwarder <name> target ssl timeout <time>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set fwlb Commands

A firewall load balancer is used to manage and control traffic that crosses a network boundary. It provides a means for securing resources on a trusted network from access by untrusted sources. Both transparent and non-transparent firewalls are supported.

Use the following commands to configure and manage firewall load balancers on the DX. To add a firewall load balancer group, see "add fwlb group" on page 18.

set fwlb

Description This command is used to enable or disable the firewall load balancer. Firewall load balancing is disabled by default.

This command does not take effect until after a `write` operation.

Syntax
```
set fwlb [disabled* |enabled]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group balance policy

Description This command is used to specify the load balancing protocol used by the firewall load balancer. The default is Round Robin. Refer to the administrator guide for descriptions of these load balancing policies.

This command does not take effect until after a `write` operation.

Syntax
```
set fwlb group <name> balance policy [roundrobin* | leastconns |
weightedleastconns | backupchain | maxconnections | weightedroundrobin>]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group healthcheck

Description This command is used to specify the interval at which health checks are made, the type of health check, the maximum number of times to attempt a health check without receiving a response, and the address of the other DX in a load-balanced pair.

The following defaults apply:

Setting	Default Value
interval with target up	20 seconds
interval with target down	10 seconds
maxtries	3
type	ICMP

This command does not take effect until after a `write` operation.

Syntax

```
set fwlb group <name> healthcheck [ interval [up | down] <time_in_sec> |
maxtries <numtries> | ip <ip_of_other_DX> | type [icmp] ]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group listen

Description This command is used to identify the interface on which the firewall load balancer should listen for traffic. Specifying the virtual IP address (VIP), port, and netmask is sufficent normally; however, if you are using a wildcard VIP, you must also specify the interface and VLAN.

The following defaults apply:

Setting	Default Value
VIP	NULL
port	0
netmask	0.0.0.0
ether	0
VLAN	0

This command does not take effect until after a `write` operation.

Syntax `set fwlb group <name> listen [vip <ip> | port <port> | netmask <netmask> | ether <ether_id> | vlan <vlan_id>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group session timeout

Description This command is used to specify the maximum amount of time a session may be idle before the session is closed by the firewall load balancer. The default is 30 minutes.

This command does not take effect until after a `write` operation.

Syntax `set fwlb group <name> session timeout <time_in_sec>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group sticky

Description This command is used to enable or disable the firewall load balancer to maintain session persistence. When this feature is enabled, the internal and external DX pair performing the firewall load balancing ensures that traffic coming through a particular firewall returns through that same firewall. This feature is disabled by default and the timeout is set to 120 minutes.

This command does not take effect until after a `write` operation.

Syntax `set fwlb group <name> sticky [[disabled* | enabled] | timeout <time_in_min>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group target host

Description This command is used to identify the specific firewall systems that are to be load-balanced by the given firewall load balancer group. Firewalls may be transparent or non-transparent.

Note that the type of firewall must match the address information provided by this command (IP address). The type of firewalls in this firewall load balancer group must be set prior to specifying other settings for the firewalls. See "set fwlb group target host type" on page 241.

The default for the maximum number of connections allowed on the firewall is zero. The default weight for the firewall is one.

This command does not take effect until after a `write` operation.

Syntax

```
set fwlb group <name> target host [ <ip> | maxconns <N> | weight <0-10> ]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set fwlb group target host type

Description This command is used to specify the type of firewall systems that are to be load-balanced by the given firewall load balancer group. Firewalls may be transparent or non-transparent. The type of firewalls must be set prior to specifying other settings for the firewalls.

This command does not take effect until after a `write` operation.

Syntax

```
set fwlb group <name> target host type [transparent | nontransparent]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Firewall Load Balancer

set gslb agent Commands

Use the `set gslb agent` commands to configure the agent to collect performance statistics for Global Server Load Balancing (GSLB). GSLB provides load balancing across multiple data centers based on any combination of the following performance metrics collected from the participating DX devices (nodes):

- Client connections
- SLB sessions
- Client throughput
- Memory usage
- CPU usage
- Target host availability
- Number of target host connections
- Round Trip Time (RTT) to the local DNS server (LDNS)

You can assign a relative weight to each metric you want to use. If a site is unavailable, GLSB automatically removes the site from consideration until it becomes available. Note the following key terms:

Term	Description
GSLB master	DX that acts as a DNS name server to reorder DNS responses based on the selected load balancing algorithm. Collects performance metrics from other GSLB nodes. May also be a GSLB node.
GSLB node	Provides performance metrics to the GSLB master, including the Round Trip Time (RTT) to the local DNS server.
GSLB agent	Runs on every DX that collects GSLB performance metrics.
GSLB group	DNS hostname that can resolve to several IP addresses. The returned IP address depends on the selected load-balancing algorithm.
GSLB resolver	Answers DNS requests received by the GSLB master. Can be configured to host DNS records or pass non-loadbalanced requests to another DNS server in the network.
Local DNS (LDNS)	A client's master DNS server or its immediate upstream proxy.
Target DNS	DNS server where non-loadbalanced requests are forwarded. May be a standard DNS server in the network, or an internal DNS server on the GSLB master.
Metric-based load balancing	Load balancing based on the current DX performance. metrics, including load, network bandwidth, and availability.
Proximity-based load balancing	Metric-based load balancing using the lowest RTT measured between each DX and the client's LDNS.

Use the following procedure to configure GSLB for metric-based load balancing.

1. Configure the GSLB agent on each remote DX that acts as a GSLB node.
2. On the DX acting as the GSLB master, do the following:
    a. Configure the GSLB agent.

b. Optionally, configure the internal DNS server.

c. Define each of the remote GSLB nodes

d. Configure a GSLB resolver.

e. Add a GSLB group to the resolver for each hostname to be load balanced. Each group specifies:

- The DX IP addresses associated with each GSLB node (and the GSLB master)
- The load-balancing policy for the hostname, and metric load balancing parameters (if any)

set gslb agent

Description Enables or disables the agent to respond to metrics requests from the GSLB master (disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set gslb agent <disabled*| enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb agent encryption

Description Enables or disables the encryption of GSLB messages (disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set gslb agent encryption <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb agent encryption key

Description Specifies a key used to encrypt GSLB messages (sent via UDP). Repeat this command to specify multiple keys. For example, if there are two GSLB masters using this remote node, each master can use a different key. You are prompted to enter the key twice. This command cannot be exported.

This command does not take effect until after a `write` operation.

Syntax `set gslb agent encryption key`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb agent listen port

Description Specifies the port number used to listen for GSLB requests (default is 3587).

This command does not take effect until after a `write` operation.

Syntax `set gslb agent listen port <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb agent listen vip

Description Specifies the IP address used to listen for GSLB requests. It can be a real IP, a floating VIP, the administration VIP, or its own independent VIP. If set to an independent VIP, it must not conflict with a VIP used by a cluster, forwarder, redirector, or the Web console.

This command does not take effect until after a `write` operation.

Syntax `set gslb agent listen vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns Commands

Use the `set gslb localdns` commands to configure the internal DNS server for GSLB.

set gslb localdns domain a

Description Adds an address record for a host in the domain. When the host parameter does not end in a period, it is not fully qualified), the name server appends the domain name to it when responding to queries. There can be only one address record for a host in a domain, however, you can have multiple aliases.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb localdns domain <domain> a <host> <ip>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain cname

Description Adds an alias for a host (i.e., add a canonical name record for alias) in the domain. The host must be one of the hosts for which an address record is already configured. If either of the host or alias does not end in a period, it is not fully qualified), the name server appends the domain name to it when responding to queries. There can be multiple aliases for a host in a domain.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb localdns domain <domain> cname <host> <alias>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain contact

Description Sets the contact email address for the domain. The contact email is not used by the name server, but is returned on request by DNS clients. The clients can then contact the administrator using this email address. The format is "`name@domain`" with the `'@'` replaced by a period (the default is "`jnpr-dx.$hostname`").

This command does not take effect until after a `write` operation.

Syntax

```
set gslb localdns domain <domain> contact <email>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain mx

Description Adds a mail exchange record that specifies the name of the mail server for a domain. When the sub-domain or mail server does not end in a period (is not fully qualified), the name server appends the domain name when responding to queries. There can be multiple mail exchange records for a domain with different priorities. Priority is a positive integer with zero being the highest priority.

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> mx <mailserver> <priority>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain ns

Description Adds a name server record for the specified domain. When the sub-domain or server name does not end in a period (is not fully qualified), the name server appends the domain name when responding to queries. There can be multiple name server records for a domain.

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> ns <servername>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain ptr

Description Adds a pointer record (for reverse DNS lookup) for an IP in the specified domain. If the host parameter does not end in a period, it is not fully qualified), the server name appends the domain name to it when responding to queries. There can be only one pointer record for an IP in a domain.

Note that for reverse lookups to work properly, a reverse "IN-ADDR.ARPA" domain must be created that has subdomains for each network, based on network number that are listed in reverse. For example, to do a reverse lookup for 192.168.0.32, add domain “0.168.192.in-addr.arpa” and add a pointer record to it:

```
% add gslb localdns domain 0.168.192.in-addr.arpa
% set gslb localdns domain 0.168.192.in-addr.arpa ptr 192.168.0.32 www.foo.com
```

Now LDNSs can look up the host name for 192.168.0.32.

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> ptr <ip> <host>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain sequence autoincrement

Description Enable or disable the incrementation of the sequence number each time the domain is changed (enabled by default).

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> sequence autoincrement <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain sequence number

Description Sets the sequence number for the domain (default is 1).

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> sequence number <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb localdns domain ttl

Description Sets the Time to Live (TTL) for the specified domain. TTL configures how long a DNS record will be cached before it needs to be removed. This TTL is used for all the Resource Records in a domain. The default TTL is 300 seconds.

This command does not take effect until after a `write` operation.

Syntax `set gslb localdns domain <domain> ttl <secs>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode Commands

Use the `set gslb remotenode` commands to identify the remote DX nodes on the GSLB master.

set gslb remotenode agentip

Description Specifies the listen IP address used by the GSLB agent on a remote DX node (refer to “set gslb agent listen vip” on page 244).

This command does not take effect until after a `write` operation.

Syntax `set gslb remotenode <name> agentip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode encryption

Description Enables or disables message encryption to match the remote node (disabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set gslb remotenode <name> encryption <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode encryption key

Description Enables or disables message encryption to match the GSLB agent setting on the remote node (refer to “set gslb agent encryption key” on page 244). You are prompted to enter the key twice.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb remotenode <name> encryption key
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode metricinterval

Description Specifies the number of seconds between requests for metrics sent from the GSLB master to each remote GSLB agent.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb remotenode <name> metricinterval <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode name

Description Changes the name of the remote DX node.

This command does not take effect until after a `write` operation.

Syntax `set gslb remotenode <name> name <new_name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode port

Description Specifies the port number used by the GSLB agent on a remote DX node (refer to “set gslb agent listen port” on page 244).

This command does not take effect until after a `write` operation.

Syntax `set gslb remotenode <name> port <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb remotenode timeout

Description Specifies the number of seconds that the GSLB master waits for a response from the remote GSLB agent. If the timeout is exceeded, the node is assumed to be unavailable, and its metrics score is set to zero.

This command does not take effect until after a `write` operation.

Syntax `set gslb remotenode <name> timeout <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver Commands

Use the `set gslb resolver` commands to configure the resolver on the GSLB master. The resolver works as a DNS proxy/filter, and can be configured to point to an external standalone DNS server or to the internal DNS server. Multiple resolvers can be created, each listening on its own virtual IP.

set gslb resolver

Description Enables or disables a GLSB resolver (disabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set gslb resolver <name> <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group dns answermode

Description Specifies whether one or multiple IP addresses are returned with each DNS request. If set to multiple, the order of the IPs depends on the load balancing policy. If the load balancing policy is "roundrobin" or "weightedroundrobin", the order is a snapshot of the current roundrobin ordering. If "random" is selected, the order is random. If "forward" is selected, this parameter is ignored and the response is determined by the target DNS. If "metric" is selected, the order is determined by each member's metric score.

If the GSLB sticky option is enabled, you must specify answermode as single (see “set gslb resolver group lba sticky” on page 254).

This command does not take effect until after a `write` operation.

Syntax

```
set gslb resolver <name> group <name> dns answermode <multiple | single>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group dns authdomainname

Description Sets the fully-qualified domain name (FQDN) for the GSLB group's authoritative domain name. This optional setting helps the local DNS identify authoritative name servers. The server and domain name (see the next command) of the authoritative server are used in the Authority section of the DNS response, and a record is added to the Additional section of the DNS response specifying the GSLB resolver's VIP and the IP address associated with authoritative server name.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> dns authdomainname <FQDN>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group dns authservername

Description Sets the fully-qualified hostname (FQHN) for GSLB group's authoritative server name. This optional setting helps the local DNS identify authoritative name servers (see the previous command).

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> dns authservername <FQHN>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group dns hostname

Description Sets the fully-qualified hostname (FQHN) for the GSLB group.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> dns hostname <FQDN>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group dns ttl

Description Sets the Time to Live (TTL) for the DNS record returned in response to a hostname lookup request (1 through 2147483647 seconds). The default is 300.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> dns ttl <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group failip

Description Sets a failure IP address to send to the local DNS when all the GSLB nodes in the group are unavailable or fail the health checks. Note the following:

- If a group has no members configured, the resolver forwards requests to the upstream authoritative DNS server and returns the response to the client.
- If all member IPs fail the health checks, and there is no failure IP set for the group, the resolver responds to queries with an answer containing no A records.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> failip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group lba policy

Description Sets the load balancing policy for a GSLB group. The default is "roundrobin". The following table describes the available load balancing policies.

Policy	Description
fixed	IPs are returned in a fixed order (no load balancing).
forward	Requests are forwarded to the target DNS (no load balancing).
metric	Performance metrics collected from each GSLB node are used to determine which IPs to return.
random	IPs are returned in a random order.
roundrobin	IPs in the group are returned in a sequential fashion, with each request getting the next IP in the group. Pings are sent to each IP in the group, one per second. If the IP fails to respond to three pings in a row, it is removed from rotation until it responds to three consecutive pings.
weightedroundrobin	Same as round roundrobin, except that the weight assigned to each IP determines the number of times the IP is served for consecutive requests before the next IP is served.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb resolver <name> group <name> lba policy <roundrobin |
weightedroundrobin | random | forward | metric>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group lba sticky

Description Enables or disables the assignment of the same DX address to consecutive requests from the same local DNS if the requests occur within a specified number of seconds (disabled by default). This affects all load balancing policies except "forward". The minimum timeout is one second. Disabling this policy may not be effective immediately due to the LDNS cache. To specify the timeout, refer to “set gslb resolver group lba sticky timeout” on page 255.

If the GSLB sticky option is enabled, you must set the `set gslb resolver group dns answermode` command to answermode single. For more information, see “set gslb resolver group dns answermode” on page 251.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb resolver <name> group <name> lba sticky <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group lba sticky max

Description Specifies the concurrent maximum number of sticky entries the DX can save. If the limit is reached, the older entry is removed.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> lba sticky max <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group lba sticky netmask

Description Specifies a netmask so that consecutive requests from different local DNSs within the netmask are given the same IP address if the requests occur within the specified timeout. The default is 255.255.255.255 (each local DNS is treated individually).

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> lba sticky netmask <netmask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group lba sticky timeout

Description Specifies the maximum number of seconds that can occur between consecutive requests from the same local DNS for both requests to receive the same DX address (the default is zero).

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> lba sticky timeout <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group member ip

Description Specifies the IP address of each DX node (member) associated with a specified group on a GSLB master. These are the load-balanced IP addresses that are returned in response to DNS queries.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> member <name> ip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group member remotenode

Description Specifies the name of the DX node used to gather performance metrics for the specified member. Specify local to indicate the GSLB master; otherwise, the name must match the name of a remote node (refer to “add gslb remotenode” on page 19).

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> member <name> remotenode <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group member weight

Description If you use weighted roundrobin load balancing, the weight (0 to 100) indicates the number of times the member address is served before the next address is used. If the member weight is 0, the member is removed from rotation. If it is non-zero, the normal load balancing calculation is performed. Weights are also used for metric-based load balancing.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> member <name> weight <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric byterate

Description Specifies the maximum allowable data rate (bytes/second) on a GSLB node, and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the byte rate is exceeded, the IP addresses associated with the node are taken out of rotation. The default rate is 125,000,000 bytes/second. You can specify "kb" or "mb" to indicate kilobytes or megabytes.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric byterate <max <N> [kb | mb] | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric connections

Description Specifies the maximum number of connections allowed on a GLSB node, and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the number of connections exceeds the specified value, the IP addresses associated with the node are taken out of rotation. The connection count includes all client and target connections for all clusters, forwarders, and redirectors, but excludes health-checking connections and SLB sessions.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric connections <max <N> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric cpuusage

Description Specifies the maximum percentage of CPU usage allowed (0 to 100) before a GSLB node is considered to be unavailable (default is 80), and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the CPU usage exceeds the specified value, the IP addresses associated with the node are taken out of rotation.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric cpuusage <max <N> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric defaults

Description Resets all metrics to the default values.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric defaults`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric memusage

Description Specifies the maximum percentage of memory usage allowed (0 to 100) before a GSLB node is considered to be unavailable (default is 80), and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the memory usage exceeds the specified value, the IP addresses associated with the node are taken out of rotation.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric memusage <max <N> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric rtt

Description Specifies the maximum acceptable RTT time (in seconds) between the GSLB node and the local DNS (calculated by ICMP pings), and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the RTT time is exceeded, the IP addresses associated with the node are taken out of rotation. The default time is 15 seconds.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric rtt <max <seconds> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric rtt count

Description Specifies the number of pings that each GSLB node sends to the local DNS to calculate the round-trip time (the default is 3). Pings are sent one second apart, and the average RTT is used. Note that the RTT count and timeout settings affect the response time of the GSLB master, which must wait for the pings to be completed.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric rtt count <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric rtt netmask

Description Specifies a netmask so that different local DNSs within the netmask are assumed to have the same RTT value. The default is 255.255.255.0 (the RTT is calculated for each LDNS).

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric rtt netmask <netmask>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric rtt timeout

Description Specifies the number of milliseconds the GSLB master waits for an RTT value from a GSLB node (the default is 15). The minimum value is 10.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric rtt timeout <milliseconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric sessions

Description Specifies the maximum number of SLB sessions allowed on a GLSB node, and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the number of SLB sessions exceeds the specified value, the IP addresses associated with the node are taken out of rotation.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric sessions <max <N> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric smoothing

Description Specifies the extent to which the collected statistics are smoothed out to alleviate the effects of sudden spikes in the data.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric smoothing <low | medium | high>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group metric targethostavailability

Description Specifies the minimum percentage (0 to 100) of target hosts that must be available on the GSLB node, and the relative weight (0 to 100) of the metric used in the load balancing calculation. If the weight is zero, the metric is not used for load balancing. If the percentage of target hosts available drops below the specified value, the IP addresses associated with the node are taken out of rotation.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> metric targethostavailability <min <N> | weight <N>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group name

Description Changes the name of a GSLB group.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> group <name> name <new_name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group servicecheck

Description Enables or disables the service check feature (default is enabled).

Syntax `set gslb resolver <name> group <name> servicecheck [disabled | enabled*]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver group servicecheck mode

Description Sets the service check mode to either ICMP (ping) or TCP connect (default is ICMP). In some cases, an IP address may respond to a ping even though the actual service a client is trying to connect to may be down. In this situation, it may be beneficial to switch to using TCP for service checking because you can specify the ports you want checked for availability.

Syntax `set gslb resolver <name> group <name> servicecheck mode <icmp* | tcp>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver listen port

Description Sets the resolver's port number (up to 65535). The default port is 53, the standard DNS port.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> listen port <n>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver listen vip

Description Sets the resolver's virtual IP for listening to public DNS requests. The VIP can be a real IP address, a floating VIP, the administration VIP, or its own independent VIP. If set to an independent VIP, it must not conflict with a VIP used by a cluster, forwarder, redirector, or the WebUI.

This command does not take effect until after a `write` operation.

Syntax `set gslb resolver <name> listen vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set gslb resolver target

Description Sets the target DNS server where DNS requests that are not load balanced are sent. Enter the IP address and port of a DNS server in the network, or enter localdns to use the internal DNS server.

This command does not take effect until after a `write` operation.

Syntax

```
set gslb resolver <name> target <ip:port | localdns>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Server Load Balancer

set health Commands

Use the `set health` command to set parameters relating to connectivity failover and scriptable health checking. The `set health script <script_name> testrun` command lets you verify that a health script is behaving properly. You can use debug messages to trace the script's logic and check the health logs to see if the health check status is being communicated properly. When the script finishes (it might not finish if it is a run-once script), you can check the exit status to see if it ran successfully. After you test a script, you can enable it for automatic execution.

set health remotehost

Description Disables or enables connectivity failover.

This command does not take effect until after a `write` operation.

Syntax

```
set health remotehost <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost host

Description Adds an IP address to health check.

This command does not take effect until after a `write` operation.

Syntax `set health remotehost host <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost interval

Description Sets the health check interval (how often to send health checks).

This command does not take effect until after a `write` operation.

Syntax `set health remotehost interval <seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost minhostsfailing

Description Sets the count for minimum number of hosts failing.

This command does not take effect until after a `write` operation.

Syntax `set health remotehost minhostsfailing <count>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost retry

Description Sets the maximum number of attempts before health check considers the host down.

This command does not take effect until after a `write` operation.

Syntax

```
set health remotehost retry <count>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost startupdelay

Description Sets the number of seconds after a reboot before health checking begins (default is 90).

This command does not take effect until after a `write` operation.

Syntax

```
set health remotehost startupdelay <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health remotehost timeout

Description Sets the number of seconds the DX waits for a health check response (default is 10).

This command does not take effect until after a `write` operation.

Syntax

```
set health remotehost timeout <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health script

Description Disables or enables a script for Scriptable Health Check.

This command does not take effect until after a `write` operation.

Syntax `set health script <script_name> <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health script interval

Description Sets the script execution interval. If a zero is set, the script will only run once. A value greater than zero specifies the run interval in seconds. The maximum value that can be set is 86,400 seconds.

This command does not take effect until after a `write` operation.

Syntax `set health script <script_name> interval <value>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health script testrun

Description Performs a test run of the health script.

This command does not take effect until after a `write` operation.

Syntax `set health script <script_name> testrun`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set health script vip

Description Sets the Script VIP. For this command, the DX will determine the most appropriate interface to alias the IP address.

This command does not take effect until after a `write` operation.

Syntax `set health script <script_name> vip <vip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover and Scriptable Health Checking

set hostname

Description Sets the host name of the DX device.

This command does not take effect until after a `write` operation.

Syntax `set hostname <hostname>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ntp Commands

Use the `set ntp` command to configure support for NTP.

set ntp

Description Disables or enables NTP support (enabled by default).

This command does not take effect until after a `write` operation.

Syntax `set ntp <down | up>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ntp server

Description Specifies the hostname or IP address for up to three NTP servers.

This command does not take effect until after a `write` operation.

Syntax `set ntp server <1-3> <hostname | ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set password

Description Use the `set password` command to set the logged-in user's password.

Individual users are only allowed to change their own password. The Administrator is allowed to change any user's password using the `set user <name>` command. For additional information, see "set user Commands" on page 310.

You are prompted for the old password before you are allowed to set the new password. No asterisks will be displayed.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set password`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

set qos Commands

Use the `set qos` commands to set the Differentiated Services Code Point/Type of Service (DSCP/ToS) values on traffic sent to the client (listen traffic) and traffic sent to the target servers. You can specify DSCP/ToS values for each cluster, forwarder, redirector, and SLB group. This feature is included in the SLB license of the product.

set ... qos mark outgoing

Description Sets the type of QoS marking for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group (default is none).

This command does not take effect until after a `write` operation.

Syntax

```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing [dscp | tos | none]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing dscp phb assured

Description Sets the Per-Hop Behavior (PHB) Assured Forwarding class and drop precedence for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group. These settings override the other PHB settings.

This command does not take effect until after a `write` operation.

Syntax

```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing dscp phb assured class <class1 | class2 | class3 | class4>
```

```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing dscp phb assured drop_precedence <low | medium | high>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing dscp phb class

Description Sets the PHB Class Selector (0-7) for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group (default is zero). This setting overrides the other PHB settings.

This command does not take effect until after a `write` operation.

Syntax

```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing dscp phb class <0-7>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing dscp phb class

Description Sets PHB Expedited Forwarding for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group. This setting overrides the other PHB settings.

This command does not take effect until after a `write` operation.

Syntax
```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing dscp phb expedited
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing dscp raw

Description Sets a raw DSCP value (0-63) for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group (default is zero). This setting overrides the Per-Hop Behavior (PHB) settings.

This command does not take effect until after a `write` operation.

Syntax
```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing dscp raw <0-63>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing tos ip-precedence

Description Sets the ToS IP precedence value (0-7) for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group (default is zero).

This command does not take effect until after a `write` operation.

Syntax
```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing tos ip-precedence <0-7>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set ... qos mark outgoing tos dtrc

Description Sets the ToS DTRC value (Delay/Throughput/Reliability/Cost) for client (listen) or server (target) traffic for a specific cluster, forwarder, redirector, or SLB group. The default is normal, (0000), indicating that DTRC is not used.

This command does not take effect until after a `write` operation.

Syntax

```
set [cluster | forwarder | redirector | slb group] <name> <listen | target> qos
mark outgoing tos dtrc <delay | throughput | reliability | cost | normal>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector Commands

Use the `set redirector` commands to set properties for the redirector. Note that the redirector must be enabled before requests will be redirected.

set redirector customurl

Description Sets the URL for redirecting. Only used when the URL method is set to “custom”.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> customurl <url string>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector description

Description Add a description to redirector `< name >`. The description is limited to 512 characters of free-form text, but cannot include new lines. This allows administrators to fully describe the redirector's usage, contact information, warnings, or any other pertinent information they deem necessary.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> description <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector

Description Disables or enables the redirector.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector dsr

Description Disables or enables the use of Direct Server Return (DSR).

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> dsr <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector host

Description Sets the redirector request host name or IP address.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> host <hostname | ip address>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector listen port

Description Sets the redirector's listen port. The default is port 80.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector listen qos

Description Sets the DSCP/ToS values on traffic sent to clients (see "set qos Commands" on page 268).

set redirector listen ssl certfile

Description Specifies the SSL certfile for redirector's listen connection.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl certfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl cipherfile

Description Specifies the name of the user-defined file containing a list of cipher suites that conform to the OpenSSL standard.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl cipherfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ciphersuite all

Description Allows all support SSL cipher suites for redirector's listen traffic. Supported cipher suites are shown in "Cipher Suites" on page 477.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl ciphersuite all`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ciphersuite common

Description Allows only the fastest cipher suites from both the strong and export groups.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl ciphersuite common`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ciphersuite export

Description Allows for the lower security cipher suites that are suitable for export.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> listen ssl ciphersuite export
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ciphersuite file

Description Allows a user-defined list of SSL cipher suites to be used to configure a redirector.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> listen ssl ciphersuite file
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ciphersuite strong

Description Allows only the highest security cipher suites that are suitable for use in the United States.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> listen ssl ciphersuite strong
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl clientauth authtype

Description Disables or enables client authentication for the redirector `< name >`. The default is "local", and provides local authorization. If none is specified, the local and remote authentications are disabled. The option ("none") may be used in situations where a client certificate needs to be forwarded to the target host.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> listen ssl clientauth authtype [local | none]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl clientauth cacertfile

Description Sets the advertised Certificate Authority (CA) file as a `< filename >` for the redirector. The `< filename >` must contain a list of one or more valid CA certificates that are self-signed or signed by:

- A well-known trusted CA
- A CA-listed in the trusted CA certificate file

All certificate entries in this file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax

```
set redirector <name> listen ssl clientauth cacertfile <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl clientauth cacrlfile

Description Sets the CA Certificate Revocation List (CRL) as `< filename >` for the redirector. The `< filename >` must be a list of one or more valid CRLs containing certificates signed by one of the CA's listed in the trusted CA certificate file. All CRL entries not corresponding to an entry in the trusted CA certificate file are ignored.

All CRLs listed in the file must be in base64-encoded format.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl clientauth cacrlfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl clientauth catrustfile

Description Sets the CA Trusted Certificate file to `< filename >` for the redirector. The `< filename >` must be a file containing a valid list of one or more root- or intermediate-CA certificates; each certificate is encoded in base64 format. If the certificate is an intermediate certificate, its root CA certificate must also be present in either a `catrustfile` or the `cacertfile`.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl clientauth catrustfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl clientauth

Description Disables or enables SSL client authentication for listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl clientauth <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl

Description Disables or enables SSL for redirector listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl autochain

Description Enables or disables SSL autochaining for redirector listen connections. When enabled, this command also sets the root certificate settings.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl autochain <disabled | enabled | rootcert>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ephkeyfile

Description Specifies the SSL ephemeral keyfile for redirector listen traffic. The ephemeral key is a debugging aid for export ciphers. The ephemeral keyfile must be a 512-bit RSA key in OpenSSL PEM (base-64) format and, if encoded, must match the password.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl ephkeyfile <ephkeyfile>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl ephkeypass

Description Specifies the ephemeral key pass phrase for redirector listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl ephkeypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl keyfile

Description Specifies the SSL keyfile for redirector listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl keyfile <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl keypass

Description Specifies the SSL key pass phrase for redirector listen traffic.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen ssl protocol

Description Specifies the SSL protocol types for redirector listen traffic:

- sslv2: SSL Version 2 only
- sslv23: SSL Version 2; SSL Version 3; TLS Version 1
- ssl3: SSL Version 3 only
- tlsv1: TLS Version 1 only

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen ssl protocol [sslv2 | sslv23 | sslv3 | tlsv1]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X			

Mode(s) Global Configuration

set redirector listen vip

Description Sets the redirector's listen Virtual IP address.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> listen vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector name

Description Changes the name of a redirector from `<name>` to `<new name>`.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> name <new name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector port

Description Sets the port for redirect requests. The default is port 443.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> port <port number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector protocol http

Description Redirects requests to use HTTP protocols.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> protocol http`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector protocol https

Description Redirects requests to use HTTPS protocols (default is https).

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> protocol https`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector target qos

Description Sets the DSCP/ToS values on traffic sent to host servers (see “set qos Commands” on page 268).

set redirector urlmethod custom

Description Redirects requests to a custom page as defined in `customurl`.

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> urlmethod custom`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set redirector urlmethod request

Description Redirects to the same page as the original request (default is request).

This command does not take effect until after a `write` operation.

Syntax `set redirector <name> urlmethod request`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set route default

Description Sets the default route.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set route default <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server

Description Enables or disables the DX server.

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax `set server <up | down>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

set server compression Commands

Use the `set server compression` commands to configure server compression.

set server compression 2k_padding

Description Disables or enables 2 KByte padding for compression to correct a problem with Internet Explorer (IE) 5.x clients when gzip compression is enabled as Accept-encoding (disabled by default). This problem was fixed in IE 6.x.

This command does not take effect until after a `write` operation.

Syntax

```
set server compression 2k_padding <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression browser

Description Sets the compression option for a specific browser (default is recommended).

This command does not take effect until after a `write` operation.

Syntax

```
set server compression browser <ie4 | ie50 | ie51 | ie55 | ie6 | ie7 | ieother |
konqueror | ns4 | ns6 | opera | other | safari> <0-3>
```

0 = no, 1 = gzip, 2 = deflate, 3 = recommended

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression browser defaults

Description Resets all the browser compression options to recommended.

This command does not take effect until after a `write` operation.

Syntax `set server compression browser default`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression cmt

Description Sets the Custom MIME Type to 1, 2, or 3.

This command does not take effect until after a `write` operation.

Syntax `set server compression cmt <1 | 2 | 3> <header>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression cmt

Description Disables or enables compression Custom MIME Type (disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set server compression cmt <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression defaults

Description Resets the compression options to their default values.

This command does not take effect until after a `write` operation.

Syntax `set server compression defaults`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression flushthreshold

Description Flush compression buffers for the first N bytes of response.

This command does not take effect until after a `write` operation.

Syntax `set server compression flushthreshold <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression force

Description Forces the use of one or all compression algorithms (default is all).

This command does not take effect until after a `write` operation.

Syntax `set server compression force <0 | 1 | 2>`

0 = all, 1 = gzip, 2 = deflate

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression http10

Description Disables or enables compression for HTTP/1.0.

This command does not take effect until after a `write` operation.

Syntax `set server compression htt10 <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression javascript

Description Disables or enables compression for application/x-javascript.

This command does not take effect until after a `write` operation.

Syntax `set server compression javascript <disabled | enabled*>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression level

Description Sets the compression level.

This command does not take effect until after a `write` operation.

Syntax `set server compression level <1 - 9>`

3 = compress with level 3

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression msoffice

Description Disables or enables compression for MS Office (i.e., application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/vnd.ms-project, and application/vnd.visio).

This command does not take effect until after a `write` operation.

Syntax `set server compression msoffice <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression octetstream

Description Disables or enables compression for application/octet-stream.

This command does not take effect until after a `write` operation.

Syntax `set server compression octetstream <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression optimization

Description Disables or enables compression for compression optimization. (No slide).

This command does not take effect until after a `write` operation.

Syntax `set server compression optimization <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression pdf

Description Disables or enables compression for application/pdf.

This command does not take effect until after a `write` operation.

Syntax `set server compression pdf <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression policy

Description Disables or enables server compression:

0 = Enable (default)

1 = Disable

This command does not take effect until after a `write` operation.

Syntax `set server compression policy <0 | 1>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression sharepoint

Description Disables or enables compression for application/x-vermeer-rpc.

This command does not take effect until after a `write` operation.

Syntax `set server compression sharepoint <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression shockwave

Description Compresses application/x-shockwave Flash.

This command does not take effect until after a `write` operation.

Syntax
```
set server compression shockwave <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server compression <text_>

Description Disables or enables compression for each type of text (CSS, HTML, and plain text are enabled by default).

This command does not take effect until after a `write` operation.

Syntax
```
set server compression <text_css | text_html | text_plain | text_xcomponent |
text_xml> <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set server customiplogheader

Description Use the `set server customiplogheader` command to set the custom HTTP header that will be added along with the client's original IP at the client's request. The header can either be a literal or a custom field in which the DX will insert the origin client's IP address. For additional information, see the "Logging" chapter of the *Installation and Administration Guide for DXOS*.

Setting `cusomiplogheader` to "X-Forwarded-For" allows you to override the `REMOTE_ADDR HTTP` variable that BEA Weblogic uses to look up client IP addresses. To do so, set "X-Forwarded-For" to the client's IP address, then set the `customiplogheader` to "X-Forwarded-For".

This command does not take effect until after a `write` operation.

Syntax
```
set server customplogheader <header>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server forwardclientcert headername

Description Sets the custom HTTP header used for SSL client certificate forwarding.

This command does not take effect until after a `write` operation.

Syntax `set server forwardclientcert headername <header>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server failover

The service-specific failover commands are listed in “Service Failover Commands” on page 479. These commands have been replaced by the commands for Unified Failover (refer to “set failover Commands” on page 215).

set server maxconns

Description Sets the maximum number of simultaneous connections that the DX can support.

This command does not take effect until after a `write` operation.

Syntax `set server maxconns <value>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server reversepath Commands

Use the `set server reversepath` commands to configure the reversepath feature.

set server reversepath

Description Disables or enables the reversepath feature (default).

This command does not take effect until after a `write` operation.

Syntax

```
set server reversepath <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server reversepath maxroutes

Description Configures the maximum number of routes that can be added with reversepath. The minimum number is one, and the maximum is 500. The default is 20.

This command does not take effect until after a `write` operation.

Syntax

```
set server reversepath maxroutes <number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set server reversepath timeout

Description Configures the timeout value for the entries added by reversepath. Routes will be deleted after this interval of inactivity. The minimum timeout value is one second, and the maximum value is 5,000 seconds (default is 45 seconds).

This command does not take effect until after a `write` operation.

Syntax

```
set server reversepath timeout <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set slb Commands

Use the set slb commands to configure the internal Server Load Balancer (SLB). The `set slb disabled` and `set slb enabled` options take effect immediately, however, a `write` operation is needed to make the change persistent. The other SLB settings take effect only after a `write` operation.

See the "Server Load Balancing" chapter of the *DX Application Acceleration Platform Installation and Administration Guide* for complete information on Server Load Balancing policies.

set slb

Description Disables or enables the Server Load Balancer (disabled by default).

This command takes effect immediately. Enter a `write` command to retain the change after the next reboot.

Syntax

```
set slb <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb advanced reset

Description When active sessions are purged, a reset can be sent to the client and/or server to indicate that the connection has been terminated (enabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set slb advanced reset <client | server> <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb failover

The service-specific failover commands are listed in "Service Failover Commands" on page 479. These commands have been replaced by the commands for Unified Failover (refer to "set failover Commands" on page 215).

set slb group advanced reset

Description When active sessions in the specified group are purged, a reset can be sent to the client and/or server to indicate that the connection has been terminated (enabled by default). This overrides the global SLB setting (refer to "set slb advanced reset" on page 292). The global option is the same as enabled.

This command does not take effect until after a `write` operation.

Syntax
```
set slb group <name> advanced reset <client | server> <disabled | enabled | global>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group <hardpaused | softpaused | unpaused>

Description Pauses or unpauses traffic for the slb group (default is unpaused). A "hard" pause terminates all existing traffic, while a "soft" pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set slb group <name> <hardpaused | softpaused | unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Server Load Balancer Configuration

set slb group healthcheck interval

Overrides the global health check intervals for when target hosts are down (default is 10 seconds), for TCP SYN (default is 5 seconds), or for when target hosts are up (default is 20 seconds).

This command does not take effect until after a `write` operation.

Syntax
```
set slb group <name> healthcheck interval <down <seconds> | syn <seconds> | up <seconds>>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group healthcheck maxtries

Description Overrides the global maximum number of health checks (default is 3).

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> healthcheck maxtries <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group healthcheck smtp

Description Enables or disables SMTP health checking for a group (disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set slb group <name | all> healthcheck smtp <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group listen qos

Sets the DSCP/ToS values on traffic sent to clients (see “set qos Commands” on page 268).

set slb group minhosts

Description Sets the minimum number of target hosts used for load balancing by priority. To set the target host priorities, refer to “set slb group target host” on page 299.

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> minhosts <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group nat

Description Sets the full or half Network Address Translation (NAT) policy for the switch group (default is full).

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name> nat <full | half>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group nat port

Description Sets the range of ports (1 to 65535) for an SLB group that are subject to NAT. Since the L4 switch can operate in DSR mode, where it may not see the packets going from the target host to the client, the L4 switch uses a timer to purge the sessions. The default port range is 1024 to 65535.

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name> nat port <end | start> <port>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group policy

Description Sets the load balancing policy for the switch group (default is roundrobin).

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name | all> policy <backupchain [revert] | leastconns | maxconns
| roundrobin | weightedleastconns | weightedroundrobin>
```

Policy	Description
backupchain [revert]	Selects the first active target host in the cluster. Target hosts must be added in order of decreasing importance. The revert option returns to the more important target hosts when they become available.
leastconns	Selects the target host with the fewest outstanding requests.
maxconns	Selects a target host sequentially based on the specified maximum number of concurrent connections.

Policy	Description
roundrobin	Selects the next active target host in the cluster. So, if there are three new requests, and three active target hosts in the cluster, each target host services one request.
weightedleastconns	Selects a target host based on the weight and current load.
weightedroundrobin	Selects a target host based on the weight. The larger the weight, the higher the probability of the server being chosen.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group priority

Description Enables or disables load balancing by priority (disabled by default). To set the target host priorities, refer to “set slb group target host” on page 299.

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> priority <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group protocol

Description Sets the protocol for the switch group (default is TCP).

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> protocol <tcp | udp>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group service

Description Specifies the service type for the group (the default is default).

This command does not take effect until after a `write` operation.

Syntax
```
set slb group <name> service <default | none | ftp | tftp>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group session timeout

Description Overrides the global session purge timeouts for one or all SLB groups.

This command does not take effect until after a `write` operation.

Syntax
```
set slb group <name | all> session timeout <ackwait | active | closewait>
<seconds>
```

- `ackwait`: Three way TCP handshake has not completed (default is 6 seconds).
- `active`: Active sessions (default is 90 seconds).
- `closewait`: Sessions terminated by the client (default is 12 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group sticky

Description Enables "stickiness" of a particular client to a server within a group (disabled by default). Stickiness results in the client always being connected to the same server (if reconnected before timeout).

This command does not take effect until after a `write` operation.

Syntax
```
set slb group <name> sticky <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group sticky failover

Description Enables or disables sticky failover for the specified SLB group. When Unified Failover is also enabled, the standby DX takes on communications with the SLB group.

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name> sticky failover <disabled | enabled*>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group sticky leader

Description Specifies whether a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group (the default is none). This creates a sticky group so that client applications with multiple protocol flows (such as TCP and UDP) can be load balanced to the same target host.

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name> sticky leader <none | <cluster | forwarder | slb group>
<name>>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group sticky softpause override

Description Specifies whether the sticky feature is used when traffic is softpaused (disabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name | all> sticky softpause override <disabled* | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group sticky timeout

Description Sets the maximum number of minutes (1 to 43200) between consecutive client requests that are bound to the same target host, for one or all groups (default is 120). This overrides the SLB global timeout.

This command does not take effect until after a `write` operation.

Syntax `set slb group <name | all> sticky timeout <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb group target host

Description Sets a new target host with a real IP address. If load balancing by priority is enabled (refer to "set slb group priority" on page 296), and all the target hosts are available, load balancing is applied only to the target hosts with the highest priority (highest priority is 1, the default). If some target hosts are unavailable, lower-priority hosts are used to meet the specified minimum number of target hosts ("set slb group minhosts" on page 294).

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> target host <ip:port> [priority <1-10>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Server Load Balancer Configuration

set slb group target host <hardpaused | softpaused | unpaused>

Description Pauses or unpauses traffic for a target host (default is unpaused). A "hard" pause terminates all existing traffic, while a "soft" pause does not affect existing traffic.

Syntax This command takes place immediately; no `write` command is needed.

```
set slb group <name> target host <ip:port> <hardpaused | softpaused | unpaused>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Server Load Balancer Configuration

set slb group target host maxconns

Description Sets the maximum number of concurrent connections per target host when the maxconn load balancing policy is in effect. Range is from 0 to 20000. Setting to zero indicates an unlimited number of concurrent connections are allowed.

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name | all> target host <ip:port | all> maxconns <number>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Server Load Balancer Configuration

set slb group target host priority

Description If load balancing by priority is enabled (refer to “set slb group priority” on page 296), and all the target hosts are available, load balancing is applied only to the target hosts with the highest priority (highest priority is 1, the default). If some target hosts are unavailable, lower-priority hosts are used to meet the specified minimum number of target hosts (“set slb group minhosts” on page 294).

This command does not take effect until after a `write` operation.

Syntax

```
set slb group <name> target host <ip:port> priority <1-10>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Server Load Balancer Configuration

set slb group target host weight

Description Sets the weight of the target host (default is 1). Weights are used if weight-based load balancing is enabled (refer to "set slb group policy" on page 295).

This command does not take effect until after a `write` operation.

Syntax `set slb group <name> target host <ip:port> weight <N>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Server Load Balancer Configuration

set slb group target qos

Description Sets the DSCP/ToS values on traffic sent to clients (see "set qos Commands" on page 268).

set slb healthcheck interval

Sets the global health check intervals for when target hosts are down (default is 10 seconds), for TCP SYN (default is 5 seconds), or for when target hosts are up (default is 20 seconds).

This command does not take effect until after a `write` operation.

Syntax `set slb healthcheck interval <down <seconds> | syn <seconds> | up <seconds>>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb healthcheck maxtries

Description Sets the global maximum number of health checks before giving up (default is 3).

This command does not take effect until after a `write` operation.

Syntax `set slb healthcheck maxtries <number>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb session timeout

Description Sets the global purge timeouts for SLB sessions.

This command does not take effect until after a `write` operation.

Syntax `set slb session timeout <ackwait | active | closewait> <seconds>`

- `ackwait`: Three way TCP handshake has not completed (default is 6 seconds).
- `active`: Active sessions (default is 90 seconds).
- `closewait`: Sessions terminated by the client (default is 12 seconds).

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set slb sticky timeout

Description Sets the global maximum number of minutes (1 to 43200) between consecutive client requests that are bound to the same target host (default is 120). This value can be overridden for specific SLB groups.

Sets the global timeout for the stickiness of a particular client to a server (default is 120 minutes).

This command does not take effect until after a `write` operation.

Syntax `set slb sticky timeout <minutes>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Server Load Balancer Configuration

set snat Commands

Use the `set snat` command to configure a Source Network Address Translation (SNAT) group or to add a member to a group.

set snat group member

Description Adds a new member to a SNAT group. The name is optional. If a name is not provided, a name starting from 1 will be allocated.

This command does not take effect until after a `write` operation.

Syntax

```
set snat group <name> member [name]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set snat group member ip

Description Sets a SNAT group member's IP address.

This command does not take effect until after a `write` operation.

Syntax

```
set snat group <name> member ip <ip address>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set snat group member netmask

Description Sets a SNAT group member's IP netmask.

This command does not take effect until after a `write` operation.

Syntax

```
set snat group <name> member netmask <netmask>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set snat group vip

Description Sets the VIP for a SNAT group.

This command does not take effect until after a `write` operation.

Syntax `set snat group <name> vip <ip>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set snat idletime

Description Sets the maximum idle time in seconds (up to 24 hours). The default is 500 seconds.

This command does not take effect until after a `write` operation.

Syntax `set snat idletime <time in seconds>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set snat maxconn

Description Sets the maximum number of connections (1 to 1000). The default is 1000.

This command does not take effect until after a `write` operation.

Syntax `set snat maxconn <number of connections>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

set sync group Commands

Use the `set sync group` command to configure a synchronization group for configuration synchronization. For each command, `<memberid>` is either the `<hostname:port>` or an `<ip:port>`. Starting with software release 4.1.15, the set sync group command is disabled on the DX 3670.

set sync group description

Description Adds a description for a synchronization group.

This command does not take effect until after a `write` operation.

Syntax

```
set sync group <name> description <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group member password

Description Prompts you to enter the password for a synchronization group member.

This command does not take effect until after a `write` operation.

Syntax

```
set sync group <name> member <memberid> password
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group member port

Description Sets the port for a synchronization group member.

This command does not take effect until after a `write` operation.

Syntax

```
set sync group <name> member <memberid> port
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

set sync group member username

Description Sets the user name for a synchronization group member (default is “juniper”).

This command does not take effect until after a `write` operation.

Syntax `set sync group <name> member <memberid> username <username>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group name

Description Renames a synchronization group member.

This command does not take effect until after a `write` operation.

Syntax `set sync group <name> name <newname>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group override

Description Enables or disables the use of a group override file (disabled by default).

This command does not take effect until after a `write` operation.

Syntax `set sync group <name> override <disabled* | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group override filename

Description Sets the name for the group override file.

This command does not take effect until after a `write` operation.

Syntax

```
set sync group <name> override filename <filename>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set sync group timeout

Description Set a synchronization group's per-member timeout.

This command does not take effect until after a `write` operation.

Syntax

```
set sync group <name> timeout <time>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set timezone

Description Use the `set timezone` command to set the server's time zone. Time zone settings are shown in Table 7.

This command does not take effect until after a `write` operation.

Syntax

```
set timezone <timezone>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Table 7: Time Zones

Time Zones				
Africa/Adibjan	America/Dominica	Antarctica/Mawson	Atlantic/Azores	Europe/Riga
Africa/Accra	America/Edmonton	Antarctica/McMurdo	Atlantic/Faeroe	Europe/Rome
Africa/Addis_Ababa	America/Eirunepe	Antarctica/Palmer	Atlantic/Jan_Mayen	Europe/Samara
Africa/Algiers	America/El_Salvador	Antarctica/South_Pole	Atlantic/Madeira	Europe/San_Marino
Africa/Asmera	America/Fortaleza	Antarctica/Syowa	Atlantic/Reykjavik	Europe/Sarajevo
Africa/Bamako	America/Glace_Bay	Antarctica/Vostok	Atlantic/South_Georgia	Europe/Simferopol
Africa/Bangui	America/Godthab	Arctic/Longyearbyen	Atlantic/St_Helena	Europe/Skopje
Africa/Banjul	America/Goose_Bay	Asia/Aden	Atlantic/Stanley	Europe/Sofia
Africa/Bissau	America/Grand_Turk	Asia/Almaty	Australia/Adelaide	Europe/Stockholm
Africa/Blantyre	America/Grenada	Asia/Amman	Australia/Brisbane	Europe/Tallinn
Africa/Brazzaville	America/Guadeloupe	Asia/Anadyr	Australia/Broken_Hill	Europe/Tirane
Africa/Bujumbura	America/Guatemala	Asia/Aqtau	Australia/Darwin	Europe/Uzhgorod
Africa/Cairo	America/Guayaquil	Asia/Aqtobe	Australia/Hobart	Europe/Vaduz
Africa/Casablanca	America/Guyana	Asia/Ashgabat	Australia/Lindeman	Europe/Vatican
Africa/Ceuta	America/Halifax	Asia/Baghdad	Australia/Lord_Howe	Europe/Vienna
Africa/Conakry	America/Havana	Asia/Bahrain	Australia/Melbourne	Europe/Vilnius
Africa/Dakar	America/Hermosillo	Asia/Baku	Australia/Perth	Europe/Warsaw
Africa/Dar_es_Salaam	America/Indianapolis	Asia/Bangkok	Australia/Sydney	Europe/Zagreb
Africa/Djibouti	America/Inuvik	Asia/Beirut	Etc/GMT	Europe/Zaporozhye
Africa/Douala	America/Iqaluit	Asia/Bishkek	Etc/GMT + 0	Europe/Zurich
Africa/El_Aaiun	America/Jamaica	Asia/Brunei	Etc/GMT + 1	Indian/Antananarivo
Africa/Freetown	America/Jujuy	Asia/Calcutta	Etc/GMT + 10	Indian/Chagos
Africa/Gaborone	America/Juneau	Asia/Choibalsan	Etc/GMT + 11	Indian/Christmas
Africa/Harare	America/La_Paz	Asia/Chongqing	Etc/GMT + 12	Indian/Cocos
Africa/Johannesburg	America/Lima	Asia/Colombo	Etc/GMT + 2	Indian/Comoro
Africa/Kampala	America/Los_Angeles	Asia/Damascus	Etc/GMT + 3	Indian/Kerguelen
Africa/Khartoum	America/Louisville	Asia/Dhaka	Etc/GMT + 4	Indian/Mahe
Africa/Kigali	America/Maceio	Asia/Dili	Etc/GMT + 5	Indian/Maldives
Africa/Kinshasa	America/Managua	Asia/Dubai	Etc/GMT + 6	Indian/Mauritius
Africa/Lagos	America/Manaus	Asia/Dushanbe	Etc/GMT + 7	Indian/Mayotte
Africa/Libreville	America/Martinique	Asia/Gaza	Etc/GMT + 8	Indian/Reunion
Africa/Lome	America/Mazatlan	Asia/Harbin	Etc/GMT + 9	Pacific/Apia
Africa/Luanda	America/Mendoza	Asia/Hong_Kong	Etc/GMT-0	Pacific/Auckland
Africa/Lubumbashi	America/Menominee	Asia/Hovd	Etc/GMT-1	Pacific/Chatham
Africa/Lusaka	America/Merida	Asia/Irkutsk	Etc/GMT-10	Pacific/Easter
Africa/Malabo	America/Mexico_City	Asia/Istanbul	Etc/GMT-11	Pacific/Efate
Africa/Maputo	America/Miquelon	Asia/Jakarta	Etc/GMT-12	Pacific/Enderbury
Africa/Maseru	America/Monterrey	Asia/Jayapura	Etc/GMT-13	Pacific/Fakaofo

Table 7: Time Zones (continued)

Time Zones				
Africa/Mbabane	America/Montevideo	Asia/Jerusalem	Etc/GMT-14	Pacific/Fiji
Africa/Mogadishu	America/Montreal	Asia/Kabul	Etc/GMT-2	Pacific/Funafuti
Africa/Monrovia	America/Montserrat	Asia/Kamchatka	Etc/GMT-3	Pacific/Galapagos
Africa/Nairobi	America/Nassau	Asia/Karachi	Etc/GMT-4	Pacific/Gambier
Africa/Ndjamena	America/New_York	Asia/Kashgar	Etc/GMT-5	Pacific/Guadalcanal
Africa/Niamey	America/Nipigon	Asia/Katmandu	Etc/GMT-6	Pacific/Guam
Africa/Nouakchott	America/Nome	Asia/Krasnoyarsk	Etc/GMT-7	Pacific/Honolulu
Africa/Ouagadougou	America/Noronha	Asia/Kuala_Lumpur	Etc/GMT-8	Pacific/Johnston
Africa/Porto-Novo	America/Panama	Asia/Kuching	Etc/GMT-9	Pacific/Kiritimati
Africa/Sao_Tome	America/Pangnirtung	Asia/Kuwait	Etc/GMT0	Pacific/Kosrae
Africa/Timbuktu	America/Paramaribo	Asia/Macau	Etc/UCT	Pacific/Kwajalein
Africa/Tripoli	America/Phoenix	Asia/Magadan	Etc/Greenwich	Pacific/Majuro
Africa/Tunis	America/Port-au-Prince	Asia/Makassar	Etc/Universal	Pacific/Marquesas
Africa/Windhoek	America/Port_of_Spain	Asia/Manila	Etc/Zulu	Pacific/Midway
America/Adak	America/Porto_Velho	Asia/Muscat	Europe/Amsterdam	Pacific/Nauru
America/Anchorage	America/Puerto_Rico	Asia/Nicosia	Europe/Andorra	Pacific/Niue
America/Anguilla	America/Rainy_River	Asia/Novosibirsk	Europe/Athens	Pacific/Norfolk
America/Antigua	America/Rankin_Inlet	Asia/Omsk	Europe/Belfast	Pacific/Noumea
America/Araguaina	America/Recife	Asia/Oral	Europe/Belgrade	Pacific/Pago_Pago
America/Aruba	America/Regina	Asia/Phnom_Penh	Europe/Berlin	Pacific/Palau
America/Asuncion	America/Rio_Branco	Asia/Pontianak	Europe/Bratislava	Pacific/Yap
America/Barbados	America/Santiago	Asia/Pyongyang	Europe/Brussels	Pacific/Pitcairn
America/Belem	America/Santo_Domingo	Asia/Qatar	Europe/Bucharest	Pacific/Ponape
America/Belize	America/Sao_Paulo	Asia/Qyzylorda	Europe/Budapest	Pacific/Port_Moresby
America/Boa_Vista	America/Scoresbysund	Asia/Rangoon	Europe/Chisinau	Pacific/Rarotonga
America/Bogota	America/Shiprock	Asia/Riyadh	Europe/Copenhagen	Pacific/Saipan
America/Boise	America/St_Johns	Asia/Saigon	Europe/Dublin	Pacific/Tahiti
America/Buenos_Aires	America/St_Kitts	Asia/Sakhalin	Europe/Gibraltar	Pacific/Tarawa
America/Cambridge_Bay	America/St_Lucia	Asia/Samarkand	Europe/Helsinki	Pacific/Tongatapu
America/Cancun	America/St_Thomas	Asia/Seoul	Europe/Istanbul	Pacific/Truk
America/Caracas	America/St_Vincent	Asia/Shanghai	Europe/Kaliningrad	Pacific/Wake
America/Catamarca	America/Swift_Current	Asia/Singapore	Europe/Kiev	Pacific/Wallis
America/Cayenne	America/Tegucigalpa	Asia/Taipei	Europe/Lisbon	SystemV/AST4
America/Cayman	America/Thule	Asia/Tashkent	Europe/Ljubljana	SystemV/AST4ADT
America/Chicago	America/Thunder_Bay	Asia/Tbilisi	Europe/London	SystemV/CST6
America/Chihuahua	America/Tijuana	Asia/Tehran	Europe/Luxembourg	SystemV/CST6CDT
America/Cordoba	America/Tortola	Asia/Thimphu	Europe/Madrid	SystemV/EST5
America/Costa_Rica	America/Vancouver	Asia/Tokyo	Europe/Malta	SystemV/EST5EDT

Table 7: Time Zones (continued)

Time Zones				
America/Cuiaba	America/Whitehorse	Asia/Ulaanbaatar	Europe/Minsk	SystemV/HST10
America/Curacao	America/Winnipeg	Asia/Urumqi	Europe/Monaco	SystemV/MST7
America/Dawson	America/Yakutat	Asia/Vientiane	Europe/Moscow	SystemV/MST7MDT
America/Danmarkshavn	America/Yellowknife	Asia/Vladivostok	Europe/Nicosia	SystemV/PST8
America/Dawson_Creek	Antarctica/Casey	Asia/Yakutsk	Europe/Oslo	SystemV/PST8PDT
America/Denver	Antarctica/Davis	Asia/Yekaterinburg	Europe/Paris	SystemV/YST9
America/Detroit	Antarctica/DumontDUrville	Asia/Yerevan	Europe/Prague	SystemV/YST9YDT

set user Commands

Use the `set user name` commands to define a user's role, enable or disable a user, and set or change a user's password.

set user

Description Disables or enables a user.

This command takes effect immediately. Changes are automatically retained after the next reboot.

Syntax

```
set user <name | all> <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set user class

Description Sets the class attribute of a user for Administrator Remote Administration.

This command takes effect immediately. Changes are automatically retained after the next reboot.

Syntax

```
set user <name | all> class <local | remote>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set user mustchange

Description The password for the account must be changed the next time that the user logs in.

This command takes effect immediately. Changes are automatically retained after the next reboot.

Syntax

```
set user <name | all> mustchange
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set user password

Description Changes the password of a user. The password must be at least five characters.

This command takes effect immediately. Changes are automatically retained after the next reboot.

Syntax

```
set user <name | all> password
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set user role

Description Assigns one or more additional roles to a user. For a description of each of the following roles, refer to “Managing User Access” on page 5.

- administrator
- network _administrator
- network_operator
- security_administrator
- security_operator
- target_operator
- user

This command has no effect on the default “admin” account or the administrative user who is making the changes.

This command takes effect immediately. Changes are automatically retained after the next reboot.

Syntax `set user <username> role <role1, role2,...>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

set vlan Commands

Use the `set vlan` command to set the virtual LAN parameters. A tag added with a specific IP address takes precedence over a range. For example, if you add:

```
% set vlan range 192.168.10.100-192.168.10.200 10
% set vlan ip 192.168.10.34  456
```

The tag for 192.168.10.34 is 456, not 10. If a conflict occurs between the tag for the source IP and destination IP, the tag for the destination IP takes precedence.

set vlan default

Description Sets the default VLAN.

This command does not take effect until after a `write` operation.

Syntax `set vlan default <tag>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set vlan ip

Description Assigns a VLAN tag to all the packets sent to or from an IP address.

This command does not take effect until after a `write` operation.

Syntax `set vlan ip <ip address> <tag>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

set vlan range

Description Assigns a VLAN tag to all the packets sent to or from a range of IP addresses.

This command does not take effect until after a `write` operation.

Syntax `set vlan range <startip-endip | all> <tag>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

Chapter 4

Show Through Write Commands

This chapter describes all the DX show commands.

show activen Commands

Description

Use the `show activen` commands to show the ActiveN configuration. These options require an ActiveN license before they can be used.

The statistics shown by the `show activen stats` command are cumulative for all running ActiveN groups. The statistics displayed are shown in Table 8.

Table 8: activen Statistics

Statistic	Description
Total Statistics	
Bytes	The total byte count received by all clients.
Packets	The total number of packets received by all clients.
Flushed	The total number of connections that have been flushed by ActiveN. Once the appliance receives a RST or a FIN from the client for an active connection, it then waits a number of seconds, and flushes the connection. The counter is then incremented.
syn	The total number of SYNs sent by all clients.
rst	The total number of RSTs sent by all clients.
fin	The total number of FINs sent by all clients.
Current Sessions	
Active	The current number of established TCP sessions.
Fin	The current number of FINs sent by the client prior to ActiveN flushing.
Reset	The current number of RSTs sent by the client prior to ActiveN flushing.

Troubleshooting these parameters depends upon the nature of the problem that is occurring. For instance, if the “active” session count is really high and increasing, but the “flushed” count is low and not increasing, this could imply there are slow client or target hosts, or there could be high latency on transactions with the DX.

By knowing what these values mean, you can keep track of what is going on in your site (primarily from the client side to the DX). Dividing these numbers by time can give you an average occurrence count of each variable in the ActiveN statistics.

show activen

Description Shows the basic ActiveN configuration parameters.

Syntax `show activen`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) ActiveN Configuration

show activen advanced

Description Shows the advanced configuration parameters.

Syntax `show activen advanced`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show activen blade

Description Used to display the blade characteristics. Using “all” will display all blades.

Syntax `show activen blade <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) ActiveN Configuration

show activen blade <ip | all> stats

Description Used to display the blade statistics. Using “all” will display all blades.

Syntax `show activen blade <ip | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show activen failover

The service-specific failover commands are listed in "Service Failover Commands" on page 479. These commands have been replaced by the commands for Unified Failover (refer to "show failover Commands" on page 405).

show activen group

Description Shows the ActiveN configuration for one or all groups. The output is different, depending on whether the command is run on the master or passive ActiveN failover device. The group name, VIP, Port, Sticky status (enabled/disabled), and Blade index and real IP address are shown in both cases. When this command is executed on the master device, the output also displays the following additional information: the total number of blades, the number of active blades, and the status (up/down), whether the device is local (yes/no) and the MAC address for each blade.

Syntax `show activen group <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) ActiveN Configuration

show activen group sticky entries

Description Shows the clients currently associated with the specified ActiveN group.

Syntax `show activen group <name> sticky entries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) United Failover

show activen group sticky failover status

Description Shows the status of stateful failover for a the specified ActiveN group, including whether stateful failover is enabled or disabled, the address of the primary standby DX, and the start and end times for the most recent full and delta synchronization on this ActiveN group.

Syntax `show activen group <name> sticky failover status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show activen group stats

Description Shows the group statistics for one or all groups.

Syntax `show activen group <name | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show activen stats

Description Used to show the overall statistics for the switch.

Syntax `show activen stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show activen status

Description Used to display the state of the switch.

Syntax `show activen status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show activen sticky timeout

Description Used to display the sticky timeout entries.

Syntax `show activen sticky timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) ActiveN Configuration

show admin Commands

Description Use the `show admin` command to show the administrative services configuration.

The options shown in Table 9 can be entered after the `show admin` command.

Table 9: show admin Options

Options	Description	See
cli	Shows the settings for the Command Line Interface (CLI).	page 320
email	Shows email server and email address information.	page 320
interface	Shows admin interface settings.	page 321
log	Shows all logging settings.	page 321
remoteauth	Shows the settings for Administrator Remote Authorization.	page 325
scp	Shows whether SCP is enabled.	page 327
snmp	Shows SNMP information.	page 328
snmp trap	Shows SNMP trap information.	page 330
soap	Shows SOAP server information	page 333
ssh	Shows whether SSH is enabled.	page 335
syslog	Shows Syslog settings.	page 335
tcpdump	Shows TCPDump settings.	page 336
telnet	Shows whether Telnet is enabled.	page 337
tftp	Shows TFTP server settings.	page 337
tsdump	Shows TSDump settings.	page 337
upgrade	Shows upgrade filenames.	page 338

Table 9: show admin Options (continued)

Options	Description	See
vip	Shows admin VIP settings.	page 339
webui	Shows admin WebUI information.	page 340

show admin cli

Description Use the `show admin cli` command to show the configuration for the Command Line Interface (CLI). `show admin cli` shows the administrator Command Line Interface (CLI) settings.

Syntax

```
show admin cli
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Global Configuration

show admin cli sessionExpireTime

Description Shows the administrator Command Line Interface (CLI) expiration time.

Syntax

```
show admin cli sessionExpireTime
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin email

Description Use the `show admin email` command to show the main/default email configuration.

This command shows the default email configuration, but not individually configurable email settings such as those set with the `set admin log`, `set admin tcpdump`, and `set admin tsdump` commands.

Syntax

```
show admin email
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin interface

Description Use the `show admin interface` command to show admin interface settings.

Syntax `show admin interface`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin log Commands

Use the `show admin log` commands to show logging configuration.

show admin log mailto

Description Shows the email address(es) that have been set up to receive logs. To configure the DX to send logs to an email address, refer to command XXXXX

Syntax `show admin log mailto1` or `show admin log mailto2`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin log method apprules memory level

Description Shows the log level for apprules logs sent to memory.

Syntax `show admin log method apprules memory level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method apprules syslog facility

Description Shows the syslog facility for apprules logs.

Syntax `show admin log method apprules syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method apprules syslog level

Description Shows the log level for apprules logs sent to a syslog server.

Syntax `show admin log method apprules syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method audit showcmd

Description Shows whether the `show` commands entered on the CLI should be logged in the audit log.

Syntax `show admin log method audit showcmd`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin log method audit syslog facility

Description Shows the syslog facility for audit logs.

Syntax `show admin log method audit syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method audit syslog level

Description Shows the log level for audit logs sent to a syslog server.

Syntax `show admin log method audit syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method health memory level

Description Shows the log level for scriptable health logs sent to memory.

Syntax `show admin log method health memory level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method health syslog facility

Description Shows the syslog facility for scriptable health logs.

Syntax `show admin log method health syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method health syslog level

Description Shows the log level for scriptable health logs sent to a syslog server.

Syntax `show admin log method health syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method system email level

Description Shows the log level for system logs sent by email.

Syntax `show admin log method system email level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method system memory level

Description Shows the log level for system logs to memory

Syntax `show admin log method system memory level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method system syslog facility

Description Shows the syslog facility for system logs.

Syntax `show admin log method system syslog facility`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log method system syslog level

Description Shows the log level for system logs sent to a syslog server.

Syntax `show admin log method system syslog level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin log status

Description Shows whether logging is enabled or disabled on the DX.

Syntax `show admin log status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Configuration

show admin remoteauth Commands

Use the `show admin remoteauth` commands to show the configuration for Administrator Remote Authentication.

show admin remoteauth

Description Shows all configuration settings for Administrator Remote Authentication.

Syntax `show admin remoteauth`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin remoteauth ldap

Description Shows all the LDAP settings or just the specified setting.

Syntax `show admin remoteauth ldap [base-dn | bind | server [1 | 2] uid | version]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin remoteauth protocol

Description Shows the authentication protocol used for Administrator Remote Authentication.

Syntax `show admin remoteauth protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin remoteauth radius server

Description Shows all the global RADIUS settings, including the authentication key, the number of retries, the IP address and port number of both servers (1 and 2), and the timeout value. You can also view a specific setting.

Syntax `show admin remoteauth radius server [1 | 2 | key | retries | timeout]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin remoteauth status

Description Shows whether Administrator Remote Authentication is disabled or enabled.

Syntax `show admin remoteauth status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin remoteauth userrole

Description Shows the default role for remote users.

Syntax `show admin remoteauth userrole`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show admin scp Commands

Use the `show admin scp` commands to show the SCP configuration.

show admin scp

Description Displays the SCP server address and user name.

Syntax `show admin scp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin scp server

Description Displays the SCP server IP address or host name.

Syntax `show admin scp server`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin scp username

Description Displays the user name for the SCP operation.

Syntax `show admin scp username`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp Commands

Use the `show admin snmp` commands to show the configuration of the Simple Network Management Protocol (SNMP).

show admin snmp

Description Use the `show admin snmp` command to show the entire SNMP configuration.

Syntax `show admin snmp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp community

Description Shows the SNMP community configuration.

Syntax `show admin snmp community`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp community ip

Description Shows the network SNMP connection status.

Syntax `show admin snmp community ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp community name

Description Shows the SNMP community name.

Syntax `show admin snmp community name`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp community netmask

Description Shows the netmask used to allow SNMP connections from the specified network.

Syntax `show admin snmp community netmask`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp contact

Description Shows the SNMP system contact.

Syntax `show admin snmp contact`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp location

Description Shows the SNMP system location.

Syntax `show admin snmp location`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp status

Description Shows whether the SNMP is up or down.

Syntax `show admin snmp status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap

Description Use the `show admin snmp trap` command to display options related to sending SNMP traps.

Syntax `show admin snmp trap`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap authfailure

Description Displays the status of authentication failure trap sending.

Syntax `show admin snmp trap authfailure`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap enterprise

Description Displays the status of enterprise-specific trap sending.

Syntax `show admin snmp trap enterprise`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap generic

Description Displays the status of the generic trap sending.

Syntax `show admin snmp trap generic`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap host

Description Displays SNMP host settings for IP addresses, community strings, and the version configured.

Syntax `show admin snmp trap host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap host [1 | 2]

Description Displays the SNMP host setting for each trap host.

Syntax `show admin snmp trap host [1 | 2]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap host [1 | 2] community

Description Displays the SNMP community string for each trap host.

Syntax `show admin snmp trap host [1 | 2] community`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap host [1 | 2] ip

Description Displays the IP address for each SNMP trap host.

Syntax `show admin snmp trap host [1 | 2] ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap host [1 | 2] version

Description Displays the SNMP version configured for each trap host.

Syntax `show admin snmp trap host [1 | 2] version`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin snmp trap threshold

Description Displays the percentage of the maximum number of client-side connections that generates a connection threshold trap, and the percentage of login failures that triggers an authentication failure trap. You can also view just one threshold.

Syntax `show admin snmp trap threshold [connection | loginfail]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin soap Commands

Use the `show admin soap` command to show the configuration of the Simple Object Access Protocol (SOAP) server. The SOAP server is used with configuration synchronization.

show admin soap

Description Shows all of the configuration parameters for the SOAP server.

Syntax `show admin soap`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Configuration Synchronization

show admin soap port

Description Shows the port number for the SOAP server.

Syntax `show admin soap port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Configuration Synchronization

show admin soap ssl

Description Shows all of the SSL configuration parameters for the SOAP server.

Syntax `show admin soap ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Configuration Synchronization

show admin soap ssl certfile

Description Shows the SSL certificate filename for the SOAP server.

Syntax `show admin soap ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Configuration Synchronization

show admin soap ssl keyfile

Description Shows the SSL key file for the SOAP server.

Syntax `show admin soap ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Configuration Synchronization

show admin soap ssl keypass

Description Shows the SSL key password for the SOAP server.

Syntax `show admin soap ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Configuration Synchronization

show admin soap status

Description Shows the status of the SOAP server.

Syntax `show admin soap status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Configuration Synchronization

show admin ssh

Description Shows whether Secure Shell (SSH) access to the DX is enabled.

Syntax `show admin ssh [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin stats history status

Description Shows whether collection of historical statistics for forwarders, clusters, and target hosts services is enabled. It also shows the number of services enabled, and the maximum number allowed.

Syntax `show admin stats history [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin syslog

Description Shows the Syslog facility and the IP address and port number of the two Syslog servers (1 and 2). You can also view just the Syslog facility or the IP address and port of one server.

Syntax `show admin syslog [facility | host [1 | 2]]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tcpdump Commands

Description Use the `show admin tcpdump` command to show the TCPDump configuration.

show admin tcpdump

Description Displays the TCPDump configuration.

Syntax `show admin tcpdump`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tcpdump capturesize

Description Displays the value used to calculate the total size of the admin filesystem.

Syntax `show admin tcpdump capturesize`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin telnet

Description Shows whether the Telnet service is up or down.

Syntax `show admin telnet [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tftp

Description Use the `show admin tftp` command to display the TFTP configuration.

Syntax `show admin tftp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tsdump Commands

Description Use the `show admin tsdump` command to display the Technical Services Dump configuration.

show admin tsdump

Description Displays the TSDump configuration.

Syntax `show admin tsdump`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tsdump filename

Description Displays the remote filename for the TSDump.

Syntax `show admin tsdump filename`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin tsdump transport

Description Displays the transport method used to send the TSDump information. The transport method can be any of SMTP, TFTP, or SCP.

Syntax `show admin tsdump transport`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin upgrade Commands

Description Use the `show admin upgrade` command to show the filename of the DX pac file (firmware) to be upgraded.

show admin upgrade

Description Shows the upgrade information.

Syntax `show admin upgrade`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin upgrade filename

Description Shows the filename of the upgrade pac file.

Syntax `show admin upgrade filename`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin upgrade transport

Description Shows the transport method used to install the new firmware.

Syntax `show admin upgrade transport`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin vip

Description Use the `show admin vip` command to show the Virtual IP Address (VIP) of the DX.

Syntax `show admin vip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui Commands

Use the `show admin webui` commands to show the settings for the Web User Interface (WebUI).

show admin webui

Description Shows the WebUI configuration.

Syntax `show admin webui`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui port

Description Shows the WebUI administration server listen port. It is possible to configure WebUI administrator to listen on an IP (10.0.20.0, for example) and use port 8090. At the same time, a cluster of target hosts may be configured to use the same IP and port (10.0.20.0:8090). When a configuration change is made that requires a restart of the multiplexing engine, a WebUI administrator page could be displayed. To prevent this from occurring, you should **NOT** use the administrator port as a cluster port. (The default listen port = 8090).

Syntax `show admin webui port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui sessionExpireTime

Description Shows the timeout for WebUI administration sessions.

Syntax `show admin webui sessionExpireTime`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui ssl

Description Shows all SSL information for the WebUI administration server.

Syntax `show admin webui ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui ssl certfile

Description Shows the SSL certificate filename for the WebUI.

Syntax `show admin webui ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui ssl keyfile

Description Shows the SSL key file for the WebUI.

Syntax `show admin webui ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui ssl keypass

Description Shows the SSL key password for the WebUI.

Syntax `show admin webui ssl keypass`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui ssl status

Description Shows whether the WebUI administration server is using SSL.

Syntax `show admin webui ssl status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show admin webui status

Description Shows whether the WebUI administration server is down (disabled) or up (enabled).

Syntax `show admin webui status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show authentication Commands

Use the `show authentication` commands to show the configuration and statistics for the authentication cache.

show authentication

Description Shows all information regarding the authentication feature.

Syntax `show authentication`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(s) Authentication

show authentication cache

Description Shows information regarding the authentication cache.

Syntax `show authentication cache`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) HTTP(s) Authentication

show authentication cache stats

Description Shows the statistics for the authentication cache.

Syntax `show authentication cache stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(s) Authentication

show boot

Description Shows the boot partition information.

Syntax `show boot`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cache Commands

Use the `show cache <name>` command to show the configuration for a named cache. If no name is specified, all caches are displayed.

show cache

Shows the configuration for one or all caches.

Syntax `show cache <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) 3G Cache

show cache stats

Description Displays cache usage statistics for a named cache. To monitor the cache usage, specify the number of seconds between each new row of statistics. Note that long URLs will be truncated.

Syntax

```
show cache <name> stats <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) 3G Cache

show cache stats <details>

Description Shows detailed statistics based on the specified criteria. The LRU is the Least Recently Used element, and the MRU is the Most Recently Used element. Where the commands take an optional `<number>` argument, the `<number>` limits the count of records. The valid range for `<number>` is 1-100, and defaults to 100.

Syntax

```
show cache <name> stats [ detail [number] | summary | object_size | content_type
| hit_count [number] | MRU [number] | LRU [number] ]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) 3G Cache

show capacity

Description Shows the DX CPU and memory usage, and the amount of interface and network traffic. To view the system capacity, specify the number of seconds between new rows of statistics. The values shown are averaged over the previous 60 seconds.

Syntax

```
show capacity <seconds>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show clock

Description Shows the time and date.

The output of the show clock command is in the following format:

```
<YYYY.MM.DD HH:MM:SS TZ>
Where YYYY = year
    MM = month
    DD = day
    HH = hour
    MM = minute
    SS = second
    TZ = timezone
```

Syntax `show clock`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

show cluster

Description Shows the cluster configuration for one or all clusters. You can see only the cluster information allowed by your role.

Syntax `show cluster [name]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

show cluster aaa audit

Description Shows whether HTTP(S) authentication auditing is disabled or enabled.

Syntax `show cluster <name> aaa audit`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication Commands

Use the `show cluster <name> aaa authentication` commands to view the HTTP(S) authentication and authorization settings for a cluster.

show cluster aaa authentication

Description Shows all of the authentication parameters that have been set for the cluster. The `stats aaa` commands require an Authentication/LDAP license.

Syntax `show cluster <name> aaa authentication`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication cache

Description Shows all of the authentication cache parameters that have been set for the cluster.

Syntax `show cluster <name> aaa authentication cache`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication cache maxage

Description Shows the maximum time that an authentication cache entry will be stored.

Syntax `show cluster <name> aaa authentication cache maxage`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication cache status

Description Shows the status of authentication cache (disabled or enabled).

Syntax `show cluster <name> aaa authentication cache status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap

Description This command shows all parameters related to the LDAP.

Syntax `show cluster <name> aaa authentication ldap`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap anonymous

Description This command shows whether anonymous access to the LDAP database is allowed.

Syntax `show cluster <name> aaa authentication ldap anonymous`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap base-dn

Description This command shows the root Distinguished Name (DN).

Syntax `show cluster <name> aaa authentication ldap base-dn`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap bind-dn

Description This command shows the bind user Distinguished Name (DN).

Syntax `show cluster <name> aaa authentication ldap bind-dn`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap gid

Description This command shows the Group ID for the cluster.

Syntax `show cluster <name> aaa authentication ldap gid`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap server

Description This command shows the IP address and port of the named LDAP server (server 1 or server 2) that will be used for the cluster.

Syntax `show cluster <name> aaa authentication ldap server <1 | 2>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap server type

Description This command shows the server type used for aaa authentication password management.

Syntax `show cluster <name> aaa authentication ldap server type`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap ssl

Description Shows the LDAP SSL status, cacertfile, and URI for the specified cluster.

Syntax `show cluster <name> aaa authentication ldap ssl [cacertfile | status | uri]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap uid

Description This command shows the user ID for the cluster.

Syntax `show cluster <name> aaa authentication ldap uid`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication ldap version

Description This command shows the LDAP protocol version that is in use.

Syntax `show cluster <name> aaa authentication ldap version`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication method

Description Shows the method of authentication that will be used for the cluster.

Syntax `show cluster <name> aaa authentication method`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication password

Description This command shows the aaa authentication password, or whether null passwords are accepted, the maximum time a password can be used, or the maximum password length.

Syntax `show cluster <name> aaa authentication password [empty_allowed | maxage | maxlength]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication protocol

Description Shows the authentication protocol.

Syntax `show cluster <name> aaa authentication protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication radius server

Description Shows all the RADIUS settings for the cluster, including the authentication key, the number of retries, the IP address and port number of both servers (1 and 2), and the timeout value. You can also view a specific setting.

Syntax `show cluster <name> aaa authentication radius server [1 | 2 | key | retries | timeout]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication realm

Description Shows realm name displayed in the login dialog box.

Syntax `show cluster <name> aaa authentication realm`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication redirect

Description Shows all the redirect settings used when a password change flag is received from the LDAP or Active Directory server. You can also view a specific setting.

Syntax `show cluster <name> aaa authentication redirect [host | protocol | status | url]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication response

Description This command is used to show the authentication HTML message that will be used for the cluster.

Syntax `show cluster <name> aaa authentication response`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso

Description This command is used to show the Single Sign-On (SSO) configuration for the cluster,including SSO status, domain, cookie name and expiration setting.

Syntax `show cluster <name> aaa authentication response`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso cookie

Description This command is used to show the Single Sign-On (SSO) cookie configuration for the cluster, including the cookie name and timeout settings.

Syntax `show cluster <name> aaa authentication sso cookie`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso cookie name

Description This command is used to show the Single Sign-On (SSO) cookie name for the cluster.

Syntax `show cluster <name> aaa authentication sso cookie name`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso cookie timeout

Description This command is used to show the Single Sign-On (SSO) cookie timeout configuration setting for the cluster.

Syntax `show cluster <name> aaa authentication sso cookie timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso domain

Description This command is used to show the Single Sign-On (SSO) domain for the cluster.

Syntax `show cluster <name> aaa authentication sso domain`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster aaa authentication sso status

Description This command is used to show whether Single Sign-On (SSO) is enabled for the cluster.

Syntax `show cluster <name> aaa authentication sso status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X	X	X

Mode(s) HTTP(S) Authentication

show cluster apprule Commands

Use the `show cluster <name> apprule` commands to view an OverDrive AppRule ruleset for a specific cluster.

show cluster apprule

Description Shows all of the AppRule configuration settings for a particular cluster.

Syntax `show cluster <name> apprule`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule limit

Description Displays the AppRule retrypost limit.

Syntax `show cluster <name> apprule limit [retrypost]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule ruleset

Description Shows the AppRule ruleset for a particular cluster.

Syntax `show cluster <name> apprule ruleset`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule stats

Description Shows all AppRule statistics for the specified cluster.

Syntax `show cluster <name> apprule stats [all]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule stats ptc

Description Shows the Page Translator Content (PTC) statistics for the specified cluster.

Syntax `show cluster <name> apprule ptc`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule stats pth

Description Shows the Page Translator Header (PTH) statistics for the specified cluster.

Syntax `show cluster <name> apprule pth [<N> | all]`

N represents the rule number.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule stats rs

Description Shows the Request Sentry (RS) statistics for the specified cluster.

Syntax
```
show cluster <name> apprule rs [M | all]
```

M represents the rule number.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule stats rth

Description Shows the Request Translator Header (RTH) statistics for the specified cluster.

Syntax
```
show cluster <name> apprule rth [M | all]
```

M represents the rule number.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster apprule status

Description Shows the AppRule status for a particular cluster (disabled or enabled).

Syntax
```
show cluster <name> apprule status
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Application Rules

show cluster balance

Description Shows all the balancing policy settings for the cluster, or just the balancing policy or the length of the URL that will be hashed to determine load balancing.

Syntax
```
show cluster <name> balance [policy [urlhash]]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Server Load Balancer

show cluster cache Commands

Use the `show cluster <name> cache` commands to view the caches associated with a cluster and the cache statistics.

show cluster cache

Description Shows the caches associated with a cluster.

Syntax

```
show cluster <name> cache
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) 3G Cache

show cluster cache stats

Description Shows target host-like statistics relating to the traffic a cluster is routing to a cache. If "`http`" is specified, only the HTTP statistics are shown.

If "`io`" is specified, only the I/O statistics are shown. If neither is specified, both sets are shown.

Syntax

```
show cluster <name> cache stats [http | io]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) 3G Cache

show cluster compression Commands

Use the `show cluster < name > compression targetcompression` commands to view compression settings on the link between the DX and the target web servers.

show cluster compression

Description Shows all the server compression settings.

Syntax `show cluster <name> compression`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression 2k_padding

Description Shows whether 2k padding is enabled for compression.

Syntax `show cluster <name> compression 2k_padding`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression browser

Description Shows the compression setting for all web browsers or a specific browser type.

Syntax `show cluster <name> compression browser [ie4 | ie5 | ie51 | ie55 | ie6 | ie7 | ieother | konqueror | ns4 | ns6 | opera | other | safari]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression cmt

Description Shows the CMT setting: 1, 2, or 3.

Syntax `show cluster <name> compression cmt [1 | 2 | 3]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression cmt status

Description Shows the compress CMT status: disabled or enabled.

Syntax `show cluster <name> compression cmt status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression flushthreshold

Description Shows if flush threshold compression is enabled.

Syntax `show cluster <name> compression flushthreshold`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression force

Description Shows if the compression algorithm is forced:

- 0 = none
- 1 = gzip
- 2 = deflate

Syntax `show cluster <name> compression force`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression http10

Description Shows if HTTP 1.0 is being compressed.

Syntax `show cluster <name> compression http10`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression javascript

Description Shows if application/x-javascript will be compressed.

Syntax `show cluster <name> compression javascript`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression msoffice

Description Shows if MS Office documents will be compressed.

Syntax `show cluster <name> compression msoffice`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression octetstream

Description Shows if application/octet-stream will be compressed.

Syntax `show cluster <name> compression octetstream`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression optimization

Description Shows if compression optimization is enabled.

Syntax `show cluster <name> compression optimization`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression policy

Description Shows if compression is enabled (set to zero).

Syntax `show cluster <name> compression policy`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression shockwave

Description Shows if application/x-shockwave Flash will be compressed.

Syntax `show cluster <name> compression shockwave`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression targetcompression encoding

Description Shows the Target Server Compression-Encoding method.

Syntax

```
show cluster <name> compression targetcompression encoding
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression targetcompression mode

Description Shows the Target Server Compression mode.

Syntax

```
show cluster <name> compression targetcompression mode
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster compression <text_>

Description Disables or enables compression for each type of text (CSS, HTML, and plain text are enabled by default).

This command does not take effect until after a `write` operation.

Syntax

```
show cluster <name> compression <text_css | text_html | text_plain |
text_xcomponent | text_xml> <disabled | enabled>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show cluster connbind

Description Shows whether connection binding for the cluster is enabled.

Syntax
```
show cluster <name> connbind [status]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster convert302protocol

Description Shows whether `http302protocol` conversion is enabled.

Syntax
```
show cluster <name> convert302protocol
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster customiplogheader

Description Shows the logging HTTP header.

Syntax
```
show cluster <name> customiplogheader
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster description

Description Shows the description information for the cluster.

Syntax
```
show cluster <name> description <description>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster dsr

Description Shows the cluster Direct Server Return (DSR) status.

Syntax `show cluster <name> dsr`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster health Commands

Use the `show cluster <name> health` commands to view the content health check settings for target servers.

show cluster health

Description Shows all health check settings.

Syntax `show cluster <name> health`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health connect

Description Shows the Layer 4 health check settings.

Syntax `show cluster <name> health connect`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health connect interval

Description Shows the Layer 4 connection check interval.

Syntax `show cluster <name> health connect interval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health connect ssl

Description Shows whether SSL health checking is enabled or disabled.

Syntax `show cluster <name> health connect ssl [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health connect timeout

Description Shows the Layer 4 timeout value; the maximum time (in seconds) that the DX will wait to complete a connection check.

Syntax `show cluster <name> health request timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request interval

Description Shows the Layer 7 health check interval.

Syntax `show cluster <name> health request interval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request resume

Description Shows the number of times the health check failed before the DX declares the target server down.

Syntax `show cluster <name> health request resume`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request returncode

Description Shows the expected health check returncode.

Syntax `show cluster <name> health request returncode`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request size

Description Shows the expected size of the health check response.

Syntax `show cluster <name> health request size`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request status

Description Shows the status of health checking.

Syntax `show cluster <name> health request status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request string

Description Shows the expected string of the health check response.

Syntax `show cluster <name> health request string`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request timeout

Description Shows the Layer 7 timeout value; the maximum time (in seconds) that the DX will wait for the last byte of the HTTP response, measured from the time that the "Get Request" was sent.

Syntax `show cluster <name> health request timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request urlpath

Description Shows the URL path to use for health check.

Syntax `show cluster <name> health request urlpath`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health request useragent

Description Shows the user agent for health check requests.

Syntax `show cluster <name> health request useragent`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster health retry

Description Shows the number of health check retries.

Syntax `show cluster <name> health retry`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show cluster httpmethod

Description Shows which HTTP methods are enabled for the Forward Proxy Accelerator, or whether a specific method is enabled.

Syntax

```
show cluster <name> httpmethod [connect | extended | webdav]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show cluster listen Commands

Use the show cluster <name> listen commands to view the settings for cluster listen traffic (between the appliance and the client browser).

show cluster listen

Description Shows the cluster listen configuration.

Syntax

```
show cluster <name> listen
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster listen interface

Description Shows the cluster listen interface.

Syntax

```
show cluster <name> listen interface
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster listen port

Description Shows the cluster listen port.

Syntax `show cluster <name> listen port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster listen qos

Description Shows the ToS/DSCP settings for client traffic from the cluster.

Syntax `show cluster <name> listen qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster listen ssl

Description Shows the configuration of the SSL listen parameters for a specific cluster. Supported cipher suites are shown in “Cipher Suites” on page 477.

Syntax `show cluster <name> listen ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl certfile

Description Shows the cluster listen SSL certfile.

Syntax `show cluster <name> listen ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl cipherfile

Description Shows the cluster listen SSL cipherlist file name.

Syntax `show cluster <name> listen ssl cipherfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl cipherlist

Description Shows the cluster listen SSL cipherlist (actual list) of cipher suites that are being used. The list includes he name, version, key exchange, authentication, encryption, and hash methods for each cipher suite.

Syntax `show cluster <name> listen ssl cipherlist`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl ciphersuite

Description Shows the cluster listen SSL cipher suite.

Syntax `show cluster <name> listen ssl ciphersuite`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth

Description Use the `show cluster < name > listen ssl clientauth` commands to show the configuration of the SSL client authentication parameters for a specific cluster.

`show cluster <name> listen ssl clientauth` shows the SSL client authentication configuration.

Syntax `show cluster <name> listen ssl clientauth`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth authtype

Description Shows the type of authentication being used.

Syntax `show cluster <name> listen ssl clientauth authtype`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth cacertfile

Description Shows the setting for the CA cert file.

Syntax `show cluster <name> listen ssl clientauth cacertfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth cacrlfile

Description Shows the setting for the CA CRL file.

Syntax `show cluster <name> listen ssl clientauth cacrlfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth catrustfile

Description Shows the setting for the CA-trusted certificate file.

Syntax `show cluster <name> listen ssl clientauth catrustfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth forwardclientcert

Description Shows all of the settings for the client authentication `forwardclientcert` feature.

Syntax `show cluster <name> listen ssl clientauth forwardclientcert`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth forwardclientcert format

Description Shows all of the settings for the client authentication `forwardclientcert` format.

Syntax `show cluster <name> listen ssl clientauth forwardclientcert format`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth forwardclientcert status

Description Shows all of the settings for the client authentication `forwardclientcert` headername.

Syntax `show cluster <name> listen ssl clientauth forwardclientcert status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl clientauth status

Description Shows the listen SSL clientauth status.

Syntax `show cluster <name> listen ssl clientauth forwardclientcert status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl ephkeyfile

Description Shows the ephemeral key file name.

Syntax `show cluster <name> listen ssl ephkeyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl keyfile

Description Shows the cluster listen SSL keyfile.

Syntax `show cluster <name> listen ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl protocol

Description Shows the cluster listen SSL protocol.

Syntax `show cluster <name> listen ssl protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen ssl status

Description Shows the cluster listen SSL status.

Syntax `show cluster <name> listen ssl status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster listen targetsdown

Description Shows the method used when all target hosts are down.

Notes:

- `finclient`: Refers to the historical behavior of allowing the client to connect and then subsequently closing down the connection with a FIN.
- `blackhole`: Refers to the current behavior of dropping all packets sent to the cluster that has all of its target hosts down.
- `redirect <url>`: Refers to the new behavior of redirecting clients with an HTTP302 reply to the new location specified in `<url>`. The URL is specified as:

  `http[s]://<server>[:port][/path/resource]`

Syntax `show cluster <name> listen targetsdown`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster listen vip

Description Shows the cluster's Virtual IP address.

Syntax `show cluster <name> listen vip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster owa

Description Shows whether Outlook Web Access (OWA) is enabled for the cluster.

Syntax `show cluster <name> owa [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show cluster sacompat Commands

Use the `show cluster<name> sacompat advanced` commands to view whether the Juniper Secure Access SSL VPN (SA) solution compatibility is configured for one or more clusters, as well as URL configuration.

show cluster <name> sacompat [status]

Description Shows whether SA compatibility is enabled and the URL values.

Syntax `show cluster <name> sacompat [status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show cluster <name> sacompat advanced

Description Shows the values of the URLs used for SA compatibility.

Syntax `show cluster <name> sacompat advanced`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show cluster <name> sacompat advanced url [1 | 2 | 3]

Description Shows the values of the specified URL or all URLs used for SA compatibility.

Syntax `show cluster <name> sacompat advanced url [1 | 2 | 3]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show cluster stats Commands

Use the show cluster stats commands to view statistics for one or all clusters.

show cluster stats

Description Shows all statistics for one or all clusters.

Syntax `show cluster <name | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

show cluster stats auth

Description Displays the authentication statistics for one or all clusters.

Syntax `show cluster <name | all> stats auth`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats health

Description Shows the health status information for the cluster. For additional information, see “show cluster stats history” on page 378.

Syntax `show cluster <name> stats health`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history

Description Shows the statistics history for a specific cluster. The statistics collected are in the categories as shown in Table 10, Table 11, Table 12, Table 13, and Table 14.

Table 10: Browsers

Browsers	
IE 6.0	Netscape 6
IE 5.5	Mozilla
IE 5.1	Opera
IE 5.0	Konquerer
IE 4.x	Safari
IE Other	None
Netscape 4	Other

Table 11: Methods

Methods			
GET	COPY	SEARCH	LABEL
HEAD	MOVE	SUBSCRIBE	MERGE
POST	LOCK	UNSUBSCRIBE	BASELINE-CONTROL
PUT	UNLOCK	X-MS-ENUMATTS	MKACTIVITY
DELETE	BCOPY	VERSION-CONTROL	BIND
TRACE	BDELETE	REPORT	MKRESOURCE
OPTIONS	BMOVE	CHECKOUT	ORDERPATCH
CONNECT	BPROPFIND	CHECKIN	ACL
PROPFIND	BPROPPATCH	UNCHECKOUT	Other
PROPPATCH	NOTIFY	MKWORKSPACE	
MKCOL	POLL	UPDATE	

Table 12: Request Errors

Request Errors	
Illegal request line too long	Illegal header line too long
Illegal method	Illegal PUT (no length)
Illegal 0.9 method	Illegal PUT (length < 0)
Illegal POST (no length)	Illegal PUT (length = 0)
Illegal POST (length < 0)	Disallowed HTTP Method
Illegal POST (length = 0)	Disallowed WebDAV Method
Illegal Header	

Table 13: Request Version

Versions
HTTP/1.1
HTTP/1.0
Other

Table 14: Content Types

Content Types	
GIF	OCTET-STREAM
JPEG	MS-WORD
HTML	MS-EXCEL
CSS	MS-POWERPOINT
XML	Custom 1
PLAIN	Custom 2
X-COMPONENT	Custom 3
JAVASCRIPT	Other
FLASH	

Syntax `show cluster <name | all> stats history`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history export

Description Shows the name of file used for the exported statistics for a cluster.

Syntax `show cluster <name> stats history export`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen

Description Shows the HTTP listen statistics for a cluster.

Syntax `show cluster <name> stats history http listen`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen browser

Description Shows all statistics by the type of browser, or the statistics for the specified time frame. The browsers monitored are shown in Table 10.

Syntax
```
show cluster <name> stats history http listen browser [day | hour | minute |
month | second | year]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen method

Description Shows the request method. The methods that are monitored are shown in Table 11.

Syntax
```
show cluster <name> stats history http listen method
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen req-err

Description Shows the illegal requests. The illegal requests are shown in Table 12.

Syntax
```
show cluster <name> stats history http listen req-err
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen request

Description Shows the number of active client requests.

Syntax
```
show cluster <name> stats history http listen request
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http listen version

Description Shows the client browser version as shown in Table 13.

Syntax `show cluster <name> stats history http listen version`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target

Description Shows the HTTP target statistics for the named cluster.

Syntax `show cluster <name> stats history http target`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target bytesin

Description Shows the target bytes from servers sorted by content type as shown in Table 14.

Syntax `show cluster <name> stats history http target bytesin`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target bytesout

Description Shows the target bytes sent to users sorted by content type as shown in Table 14.

Syntax
```
show cluster <name> stats history http target bytesout
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target content

Description Shows the types of content handled sorted by content type as shown in Table 14.

Syntax
```
show cluster <name> stats history http target content
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target decompression

Description Shows historical statistics for decompression.

Syntax
```
show cluster <name> stats history http target decompression [performed |
failure] [hour | day | month | year]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history http target responsecode

Description Shows the quantity of each type of response code handled. (Response Code 101, etc.).

Syntax
```
show cluster <name> stats history http target responsecode
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history io listen

Description Shows the client-side I/O statistics for the cluster, including:

- Bytes In (requests from clients)
- Bytes Out (responses to clients)
- Current Client Connections
- Total Client Connections
- Refused Client Connections

Syntax `show cluster <name> stats history io listen`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history io target

Description Shows the server-side I/O statistics for the cluster, including Bytes In (requests from clients) and Bytes Out (responses to clients).

Syntax `show cluster <name> stats history io target`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history ssl

Description Shows the SSL statistics for the cluster including the number of:

- New Sessions
- Re-used Sessions
- Sessions with Strong Encryption
- Sessions with Export Encryption
- Sessions using Version SSLv2
- Sessions using Version SSLv3
- Sessions using Version TLSv1
- Sessions using Version Other

Syntax `show cluster <name> stats history ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats history status

Description Shows the status of the historical statistics feature (disabled or enabled).

Syntax `show cluster <name> stats history status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster stats http

Description Displays the HTTP statistics for one or all clusters.

Syntax `show cluster <name | all> stats http`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

show cluster stats io

Description Displays the I/O, HTTP, and SSL statistics for one or all clusters.

Syntax `show cluster <name | all> stats io`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

show cluster stats ssl

Description Displays the SSL statistics for one or all clusters.

Syntax `show cluster <name | all> stats ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

show cluster sticky Commands

Use the `set cluster <name> sticky` commands to view bindings between clients and target severs.

show cluster sticky

Description Shows the entire sticky configuration for the cluster.

Syntax `show cluster <name> sticky`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster sticky clientip

Description Shows the sticky timeout, the cluster, forwarder, or SLB group that leads this cluster, and the clusters, forwarders, and SLB groups that follow this cluster. You can also show just the timeout, leader, or followers.

When a “leader” is configured, a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group. This allows client applications with multiple protocol flows (such as TCP and UDP) to be load balanced to the same target host. The sticky method must be clientip.

Syntax `show cluster <name> sticky clientip [leader | followers | timeout]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster sticky clientip entries

Description Shows the clients currently associated with each target host.

Syntax `show cluster <name> sticky clientip entries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster sticky cookie

Description Shows all the cookie-based sticky configuration settings, or just the expire time, mask, or passheader.

Syntax `show cluster <name> sticky cookie [expire | mask | passheader]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster sticky failover status

Description Shows the status of stateful failover for a the specified Cluster service, including whether stateful failover is enabled or disabled, the address of the primary standby DX, and the start and end times for the most recent full and delta synchronization on this Cluster.

Syntax `show cluster <name> sticky failover status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show cluster sticky method

Description Shows the sticky method configuration.

Syntax `show cluster <name> sticky method`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target Commands

Use the `set cluster < name > target` commands to view the target host settings for a cluster.

show cluster target

Description Shows the cluster target configuration and local IP.

Syntax `show cluster <name> target`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target host <ip:port>

Description Shows the status, maximum connections, and weight for the specified target host. You can also view just the status, maximum connections, or weight.

Syntax `show cluster <name> target host <ip:port> [maxconnections | status | weight]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target host <ip:port | all> stats

Description Use the `show cluster <name> target host <ip:port | all> stats` command to display the I/O, HTTP or SSL statistics for a specific target host or for all target hosts in a cluster.

Syntax

```
show cluster <name> target host <ip:port | all> stats
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history

Description Use the `show cluster <name> target host <ip:port | all> stats history` command to display the history statistics for a specific target host or for all target hosts.

Syntax

```
show cluster <name> target host <ip:port | all> stats history
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http

Description Shows all of the HTTP statistics for a cluster's target host.

Syntax

```
show cluster <name> target host <ip:port | all> stats history http
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http bytesin

Description Shows the number of bytes from the target host sorted by content type as shown in Table 14.

Syntax `show cluster <name> target host <ip:port | all> stats history http bytesin`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http bytesout

Description Shows the number of bytes sent to users sorted by content type as shown in Table 14.

Syntax `show cluster <name> target host <ip:port | all> stats history http bytesout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http content

Description Shows the types of content handled sorted by content type as shown in Table 14.

Syntax `show cluster <name> target host <ip:port | all> stats history http content`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http responsecode

Description Shows the quantity of each type of response code handled. (Response Code 101, etc.).

Syntax `show cluster <name> target host <ip:port | all> stats history http responsecode`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history http target decompression

Description Shows the historical statistics for Decompression for a specific target host.

Syntax

```
show cluster <name> target host <ip:port | all> stats history http target
decompression [performed | failure] [seconds | minutes]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port> stats history io

Description Shows all the I/O statistics for a cluster's target host, or just the statistics for last 60 minutes or seconds.

Syntax

```
show cluster <name> target host <ip:port> stats history io [minutes | seconds]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats history ssl

Description Shows the SSL statistics for the target host including the number of:

- New Sessions
- Reused Sessions
- Sessions with Strong Encryption
- Sessions with Export Encryption
- Sessions using Version SSLv2
- Sessions using Version SSLv3

- Sessions using Version TLSv1
- Sessions using Version Other

Syntax `show cluster <name> target host <ip:port | all> stats history ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats http

Description Displays the HTTP statistics for a target host or for all target hosts in a cluster.

Syntax `show cluster <name> target host <ip:port | all> stats http`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats io

Description Displays the I/O statistics for a target host or for all target hosts in a cluster.

Syntax `show cluster <name> target host <ip:port | all> stats io`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster target host <ip:port | all> stats ssl

Description Displays the SSL statistics for a target host or for all target hosts in a cluster.

Syntax `show cluster <name> target host <ip:port | all> stats ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Performance Monitoring

show cluster target localip

Description Shows the local IP setting for the cluster.

Syntax `show cluster <name> target localip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target name

Description Shows the target cluster name.

Syntax `show cluster <name> target name`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target qos

Description Shows the ToS/DSCP settings for traffic sent to the cluster.

Syntax `show cluster <name> target qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster target ssl

Description Use the `show cluster < name > target ssl` commands to show the SSL target configuration of a cluster.

`show cluster <name> target ssl` shows the target server SSL configurations.

Supported cipher suites are shown in "Cipher Suites" on page 477.

Syntax

```
show cluster <name> target ssl
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl certfile

Description Shows the target server SSL certfile.

Syntax

```
show cluster <name> target ssl certfile
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl cipherlist

Description Shows the cluster listen SSL cipherlist (actual list) of cipher suites that are being used. Showing the cipherlist will print out a detailed line for each cipher suite, showing the name, version, key exchange, authentication, encryption, and hash methods.

Syntax

```
show cluster <name> target ssl cipherlist
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl ciphersuite

Description Shows the target server SSL cipher suite.

Syntax `show cluster <name> target ssl ciphersuite`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl keyfile

Description Shows the target server SSL keyfile.

Syntax `show cluster <name> target ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl protocol

Description Shows the target server SSL protocol.

Syntax `show cluster <name> target ssl protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl status

Description Shows the target server SSL status.

Syntax `show cluster <name> target ssl status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target ssl timeout

Description Shows the target server SSL timeout.

Syntax `show cluster <name> target ssl timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show cluster target status

Description Shows the health of the target server based upon Layer 7 health check.

Syntax `show cluster <name> target status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster transparency

Description Shows whether client IP transparency is enabled.

Syntax `show cluster <name> transparency`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show cluster weblog Commands

Use the `show cluster <name> weblog` commands to view the Web log settings.

show cluster weblog

Description Shows the weblog settings for the cluster.

Syntax `show cluster <name> weblog`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch

Description Shows all of the configuration parameters associated with the Web Log batch feature.

Syntax `show cluster <name> weblog batch`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch compression

Description Shows whether the Web Log will be sent to the Syslog host in compressed form or native format.

Syntax `show cluster <name> weblog batch compression`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch copy

Description Shows both the copy size and the copy time for Web Log batch storage.

Syntax `show cluster <name> weblog batch copy`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch copy interval

Description Shows the intervals at which the Web Log will be sent to the Syslog host.

Syntax `show cluster <name> weblog batch copy interval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch copy size

Description Shows the size of the compressed file to copy (the size of the two data buffers), and the total remaining memory available for Web Log batch storage.

Syntax `show cluster <name> weblog batch copy size`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch copy time

Description Shows the times when the Web Log will be transmitted to the configured Syslog server.

Syntax `show cluster <name> weblog batch copy time`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch failure

Description Shows the Web Log failure settings for the cluster.

Syntax `show cluster <name> weblog batch failure`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch failure retryinterval

Description Shows the retry interval (in seconds) in case of copy failure.

Syntax `show cluster <name> weblog batch failure retryinterval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch host

Description Shows the host where the Web Log will be copied.

Syntax `show cluster <name> weblog batch host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch scp

Description Shows all of the configuration parameters associated with the remote SCP target directory.

Syntax `show cluster <name> weblog batch scp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch scp directory

Description Shows the remote SCP target directory.

Syntax `show cluster <name> weblog batch scp directory`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch scp keyfile

Description Shows the (non-password protected) private key.

Syntax `show cluster <name> weblog batch scp keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog batch scp username

Description Shows the remote SCP username.

Syntax `show cluster <name> weblog batch scp username`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog delimiter

Description Shows the delimiter used for the Web Log.

Syntax `show cluster <name> weblog delimiter`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog destination

Description Shows the destination for the Web Log.

Syntax `show cluster <name> weblog destination`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog format

Description Shows the currently selected format for the Web Log.

Syntax `show cluster <name> weblog format`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog status

Description Shows if cluster logging is disabled or enabled.

Syntax `show cluster <name> weblog status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog syslog

Description Shows all parameters for the Web Log Syslog function.

Syntax `show cluster <name> weblog syslog`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog syslog host

Description Shows cluster Web Log Syslog log host address.

Syntax `show cluster <name> weblog syslog host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show cluster weblog syslog port

Description Shows cluster Web Log Syslog port.

Syntax `show cluster <name> weblog syslog port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Performance Monitoring

show commands

Description Shows a hierarchical list of all CLI commands.

Syntax `show commands`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show config

Description Shows the configuration in memory.

Syntax `show config`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show dashboard

Description Shows a summary of the overall health and performance of the DX, including VIP and target server health status, connections count, and byte savings.

Syntax `show dashboard`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show dns Commands

Use the `show dns` commands to show the Domain Name Service (DNS) options.

show dns domain

Description Shows the name service domain.

Syntax `show dns domain`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show dns server

Description Shows the IP addresses of all three name servers or a specific server.

Syntax `show dns server [1-3]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show ether

Description Shows all interface settings for one or all Ethernet interfaces, or just one setting for a specific interface. The following is a sample output for the ether 0 interface:

```
dx% show ether 0
ether0: IP address = 10.0.61.150  netmask = 255.255.255.0
ether0: Broadcast = 10.0.61.255
ether0: MAC = 00:30:48:72:58:34 VMAC = (unconfigured) MTU = 1500 ether0 media:
autoselect (100baseTX full-duplex) Status: active
ether0 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] 1000baseTX full-duplex
  [6] 1000baseTX
  [7] autoselect
```

The Maximum Transmission Unit (MTU) should be set to 1500 for the Ethernet.

DO NOT change this value unless your switch and network are configured to work with a different MTU.

Syntax `show ether [<n> [ip | mac | media | mtu | netmask | subnet | vmac]]`

Where `<n>` is the interface number, such as 0 or 1.

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show failover Commands

Use the `show failover` commands to show the Unified Failover settings,

show failover

Description Shows all configuration settings for Unified Failover.

Syntax `show failover`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover advanced

Description Shows one or all advanced settings.

Syntax `show failover advanced [missedcount | pollinterval | serviceinterval]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

set failover discovery

Description Shows the interface and port used to discover the other peers enabled for Unified Failover, or just the interface or port.

Syntax `show failover discovery [interface | port]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover forcemaster

Description Shows whether the forcemaster setting is enabled.

Syntax `show failover forcemaster`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover linkfail

Description Shows whether failover is triggered by a link failure on one or all interfaces.

Syntax `show failover linkfail [ether <N> status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover listen

Description Shows the port used to listen for Active and Standby packets.

Syntax `show failover listen [port]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover nodeid

Description Shows the node ID setting (a number or "auto").

Syntax `show failover nodeid`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover peer

Description Shows the listen port number and status for one or all remote static peers, or just the port or status of a specific peer.

Syntax `show failover peer [<ip> [listen | status]]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover stateful stats

Description Shows runtime statistics and information for a DX, including the total number of packets received and sent successfully for both full and delta synchronization, and the total number of full synchronization requests sent and received (successful and unsuccessful).

Syntax `show failover stateful stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show failover stateful status

Description Shows a high-level view of stateful failover for a DX. It displays whether stateful failover is enabled or disabled, the services that being synchronized (ActiveN, SLB, Server), the address of the primary standby DX, and the start and end times for the most recent full and delta synchronization procedures. Note that this information is *not* displayed on a cluster or group basis.

Syntax `show failover stateful status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show failover stateful syncinterval

Description Shows the currently configured interval at which the standby DX is synchronized with the master DX.

Syntax `show failover stateful syncinterval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show failover stats

Description Shows the general or advanced Unified Failover statistics, including the supported services and the amount of time spent in each mode (master, standby, discovery, and idle).

Syntax `show failover stats [advanced]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover status

Description Shows whether Unified Failover is enabled, the amount of time running, the node ID, and the current mode (master, standby, discovery, or idle).

Syntax `show failover status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show failover vmac

Description Shows the VMAC status (enabled/disabled) and VMAC ID for one or all interfaces. N is the number of the interface, such as 0 or 1.

Syntax `show failover vmac [ether <N> id | ether <N> status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Unified Failover

show file

Description Shows the contents of a file (same as the `display file` command).

Syntax `show file <filename>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show flash

Description Shows the total, used, and available Flash disk storage for the active partition,

Syntax `show flash`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show floatingvip

Description Shows all of the floating VIP addresses.

Syntax `show floatingvip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show forwarder Commands

Use the `show forwarder` commands to show the forwarder configuration. A forwarder is used to forward non-HTTP TCP traffic (such as SMTP traffic).

show forwarder

Description Shows information for one or all forwarders.

Syntax `show forwarder [<name>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

show forwarder balance

Description Shows all information related to the current load balancing policy for the forwarder.

Syntax `show forwarder <name> balance`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

show forwarder balance policy

Description Shows the current load balancing policy for the forwarder.

Syntax `show forwarder <name> balance policy`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					X

Mode(s) Global Configuration

show forwarder description

Description Shows the description information for a forwarder.

Syntax `show forwarder <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

show forwarder dsr

Description Shows the Direct Server Return (DSR) mode for a forwarder. Direct Server Return (DSR): A configuration where requests from the DX to the server are returned by the server directly to the client, rather than using the DX to pass the response to the client.

Syntax `show forwarder <name> dsr`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder health

Description Shows the Layer 7 health check settings.

Syntax `show forwarder <name> health`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show forwarder health connect

Description Shows the Layer 4 connection check settings.

Syntax `show forwarder <name> health connect`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show forwarder health connect interval

Description Shows the Layer 4 connection check interval.

Syntax `show forwarder <name> health connect interval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show forwarder health connect timeout

Description Shows the Layer 4 timeout value; the maximum time (in seconds) that the DX will wait to complete a connection check.

Syntax
```
show forwarder <name> health request timeout
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show forwarder health retry

Description Shows the number of health check retries.

Syntax
```
show forwarder <name> health retry
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Health Checking

show forwarder listen

Description Displays the entire listen configuration for the forwarder, or just the specified setting.

Syntax
```
show forwarder <name> listen [interface | port | qos | ssl [certfile |
cipherfile | cipherlist | ciphersuite | clientauth | ephkeyfile | keyfile |
protocol | status] | vip]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder stats

Description Displays all statistics for one or all forwarders, or just the I/O or SSL statistics.

Syntax `show forwarder <name | all> stats [io | ssl]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder sticky

Description Shows the entire sticky configuration for the forwarder.

Syntax `show forwarder <name> sticky`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder sticky clientip

Description Shows the clients currently associated with each target host (the sticky entries), the sticky timeout, the cluster, forwarder, or SLB group that leads this forwarder, and the clusters, forwarders, and SLB groups that follow this forwarder. You can also show just the sticky entries, timeout, leader, or followers.

When a “leader” is configured, a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group. This allows client applications with multiple protocol flows (such as TCP and UDP) to be load balanced to the same target host. The sticky method must be clientip.

Syntax `show forwarder <name> sticky clientip [entries | followers | leader | timeout]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder sticky failover status

Description Shows the status of stateful failover for a the specified Forwarder service, including whether stateful failover is enabled or disabled, the address of the primary standby DX, and the start and end times for the most recent full and delta synchronization on this Forwarder.

Syntax `show forwarder <name> sticky failover status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show forwarder sticky method

Description Shows the sticky method configuration.

Syntax `show forwarder <name> sticky method`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder target

Description Displays the local IP address, SSL configuration, and QoS setting used for all target hosts in a forwarder, as well as the status, weight, and maximum connections for each target host.

Syntax `show forwarder <name> target`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder target host

Description Shows the status, maximum connections, and weight for one or all target hosts in a forwarder. You can also view just the status, maximum connections, or weight.

Syntax `show forwarder <name> target host [<ip:port> | all [maxconnections | status | weight]]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder target host stats

Description Shows the I/O statistics for one or all target hosts in a forwarder.

Syntax `show forwarder <name> target host <ip:port | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder target localip

Description Shows the local IP address used for communication with all target hosts in this forwarder.

Syntax `show forwarder <name> target localip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder target qos

Description Shows the ToS/DSCP settings for traffic sent to the target hosts.

Syntax `show forwarder <name> target qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show forwarder target ssl

Description Shows the SSL configuration for all target hosts in a forwarder, or a specific SSL setting.

Syntax
```
show forwarder <name> target ssl [certfile | cipherfile | cipherlist |
ciphersuite | keyfile | protocol | status | timeout]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show forwarder target status

Description Shows the status of each target host in a forwarder.

Syntax
```
show forwarder <name> target status
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X		X	X

Mode(s) Global Configuration

show fwlb Commands

Use the show fwlb commands to view the Firewall Load Balancer configuration.

show fwlb group

Description Displays selected or all configuration information for Firewall Load Balancer groups. Firewalls associated with a specified group, statistics for the specified group, active sessions and their persistence status for the group, balance policy used, and health check configuration can all be presented together or individually.

Syntax
```
show fwlb group <name> [balance policy | healthcheck | session | session timeout
| stats | sticky | sticky timeout | target host]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show fwlb status

Description Shows the status of the Firewall Load Balancer.

Syntax `show fwlb status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	

Mode(s) Global Configuration

show gslb Commands

Use the `show gslb` command to show the Global Server Load Balancer (GSLB) configuration.

show gslb agent

Description Shows the GSLB agent configuration, or just the specified setting.

Syntax `show gslb agent [encryption [key | status] | listen [port | vip]]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show gslb agent stats

Description Shows the GSLB agent statistics.

Syntax `show gslb agent stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show gslb localdns

Description Shows the internal DNS server configuration on the GSLB master.

Syntax `show gslb localdns`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Server Load Balancer

show gslb localdns domain

Description Shows the configuration of one or all domains in the internal DNS server on the GSLB master.

Syntax `show gslb localdns domain [<domain>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Server Load Balancer

show gslb remotenode

Description Shows one or all remote node definitions on the GSLB master.

Syntax `show gslb remotenode [<name>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show gslb resolver

Description Shows the configuration for one or all resolvers on the GSLB master.

Syntax `show gslb resolver [name]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show gslb resolver group servicecheck

Description Shows the basic configuration parameters for servicechecking. These parameters include servicecheck status, mode, and TCP ports.

Syntax `show gslb resolver <name> group <name> servicecheck`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Server Load Balancer

show gslb resolver group servicecheck mode

Description Shows whether the servicecheck mode is set to ICMP or TCP.

Syntax `show gslb resolver <name> group <name> servicecheck mode`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Server Load Balancer

show gslb resolver group servicecheck status

Description Shows whether the servicechecking feature is enabled or disabled.

Syntax `show gslb resolver <name> group <name> servicecheck status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Server Load Balancer

show gslb resolver group servicecheck tcp port

Description Shows the ports included in the TCP service check.

Syntax `show gslb resolver <name> group <name> servicecheck tcp port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	

Mode(s) Global Server Load Balancer

show gslb resolver stats

Description Shows the statistics for a resolver on the GSLB master. The statistics include the requests, replies, and errors for TCP, UDP, and both combined, as well as the number of each type of DNS request. To view a line of statistics every N seconds, specify the number of seconds.

Table 15: GSLB Resolver Statistics—Shown for TCP, UDP, and Totals

Statistic	Description
Requests	Number of requests received from a local DNS.
Replies	Replies from the resolver (to the local DNS and target DNS).
Forwards	Requests forwarded to the target DNS server.
Replies from DNS server	Replies from the target DNS server.
Errors	DNS error messages generated by the resolver.

Table 16: DNS Request Types

Statistic	Description
A	Number of A record requests made to the resolver.
NS	Number of NS record requests made to the resolver.
CNAME	Number of CNAME record requests made to the resolver
SOA	Number of SOA record requests made to the resolver
PTR	Number of PTR record requests made to the resolver
MX	Number of MX record requests made to the resolver
Other	Number of other valid DNS requests made to the resolver

Syntax

```
show gslb resolver <name> stats [<seconds>]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show gslb resolver group stats

Description Shows the statistics for a specific GSLB group. To view a line of statistics every N seconds, specify the number of seconds.

Table 17: GSLB Group Statistics

Statistic	Description
Total Requests	Number of A or CNAME requests handled by the group
Pending Requests	Pending requests (generally waiting for an RTT response)
Total Replies	Total number of DNS replies generated by this group
Normal Replies	Number of DNS answers with members in them
FailIP Replies	Number of DNS answers containing only the failure IP address
Empty Replies	Number of empty DNS answers
Errors	Number of internal errors.

Syntax `show gslb resolver <name> group <name> stats [<seconds>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Server Load Balancer

show health Commands

Description Use the `show health` command to show parameters relating to connectivity failover.

show health remotehost

Description Shows all of the configurable parameters associated with remote host health check, or just the target hosts, the health check interval, the minimum number of hosts to fail before starting failover, the retry count, the health checking delay after a reboot, the status (enabled/disabled), and the timeout for a response to a health check..

Syntax `show health remotehost <host | interval | minhostsfailing | retry | startupdelay | status | timeout>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show health script <script_name | all> interval

Description Shows the interval at which the named script (or all scripts) is set to run.

Syntax `show health script <script_name | all> interval`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show health script <script_name | all> name

Description Shows the name of the named script or the names of all currently installed scripts.

Syntax `show health script <script_name | all> name`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show health script <script_name | all> stats

Description Shows the statistics for the named script (or all scripts).

Syntax `show health script <script_name | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show health script <script_name | all> status

Description Shows the status of the named script or all scripts (disabled or enabled).

Syntax `show health script <script_name | all> status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show health script <script_name | all> vip

Description Shows the VIP address for the named script (or all scripts).

Syntax `show health script <script_name | all> vip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Connectivity Failover

show hostname

Description Shows the DX host name.

Syntax `show hostname`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show license Commands

Description Use the `show license` command to show the data needed for license key generation.

show license

Description Shows details about the DX license.

Syntax `show license`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show license data

Description Shows the data needed for license key generation.

Syntax
```
show license data
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

show log Commands

Description Use the `show log` commands to show entries from the Apprule, Audit, and System logs.

show log apprule

Description Shows events from the Apprule log.

Syntax
```
show log apprule
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Application Rules

show log audit

Description Shows administrative actions recorded in the Audit log.

Syntax
```
show log audit
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Application Rules

show log health script

Description Shows events logged from health scripts.

Syntax
```
show log health script
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Application Rules

show log system

Description Shows the System log.

Syntax `show log system`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Application Rules

show loginbanner

Description Use the `show loginbanner` command to the display the current login banner with the appropriate substitutions. This banner must be previously set using the command, “capture loginbanner” on page 26.

Syntax `show loginbanner`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show ntp

Description Shows all Network Time Protocol (NTP) settings, the IP address or host name of one or all servers, or just the NTP status (up or down).

Syntax `show ntp [server [1-3] | status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show ntpq

Description Shows the results of an NTP server query. Uses a mode 6 control message format.

Syntax `show ntpq`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector Commands

Description Use the `show redirector <name>` commands to show the configuration for a specific redirector.

show redirector

Description Shows the complete redirector configuration.

Syntax `show redirector <name>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector customurl

Description Shows the custom URL setting for the redirector.

Syntax `show redirector <name> customurl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector description

Description Shows the description for the redirector.

Syntax `show redirector <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector dsr

Description Shows the DSR status, i.e., if DSR is disabled or enabled.

Syntax `show redirector <name> dsr`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector host

Description Shows the redirect host name or IP address for the redirector.

Syntax `show redirector <name> host`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector listen

Description Shows the redirector listen configuration.

Syntax `show redirector <name> listen`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector listen interface

Description Shows the redirector listen interface.

Syntax `show redirector <name> listen interface`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector listen port

Description Shows the redirector listen port.

Syntax `show redirector <name> listen port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector listen qos

Description Shows the ToS/DSCP settings for client traffic from the redirector.

Syntax `show redirector <name> listen qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector listen ssl

Description Shows the redirector listen SSL configuration. Supported cipher suites are shown in “Cipher Suites” on page 477.

Syntax `show redirector <name> listen ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl certfile

Description Shows the redirector listen SSL certfile.

Syntax `show redirector <name> listen ssl certfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl cipherfile

Description Shows the cluster listen SSL cipherlist file name.

Syntax `show redirector <name> listen ssl cipherfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl cipherlist

Description Shows the cluster listen SSL cipherlist (actual list) of cipher suites that are being used. Showing the cipherlist will print out a detailed line for each cipher suite, showing the name, version, key exchange, authentication, encryption, and hash methods.

Syntax `show redirector <name> listen ssl cipherlist`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl ciphersuite

Description Shows the redirector listen SSL cipher suite.

Syntax `show redirector <name> listen ssl ciphersuite`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl clientauth

Description Shows the listen SSL clientauth settings.

Syntax `show redirector <name> listen ssl clientauth`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl ephkeyfile

Description Shows the redirector listen SSL ephemeral keyfile.

Syntax `show redirector <name> listen ssl ephkeyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl keyfile

Description Shows the redirector listen SSL keyfile.

Syntax `show redirector <name> listen ssl keyfile`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl protocol

Description Shows the redirector listen SSL protocol.

Syntax `show redirector <name> listen ssl protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen ssl status

Description Shows the redirector listen SSL status.

Syntax `show redirector <name> listen ssl status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show redirector listen vip

Description Shows the redirector Virtual IP address.

Syntax `show redirector <name> listen vip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector port

Description Shows the port where requests will be redirected.

Syntax `show redirector <name> port`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector protocol

Description Shows the protocol that will be used to redirect requests.

Syntax `show redirector <name> protocol`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector stats

Description Shows the I/O and SSL statistics for the redirector.

Syntax `show redirector <name> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector stats io

Description Shows the I/O statistics for the redirector.

Syntax `show redirector <name> stats io`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector stats ssl

Description Shows the SSL statistics for the redirector.

Syntax `show redirector <name> stats ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector status

Description Shows the status of the redirector, i.e., if the redirector is disabled or enabled.

Syntax `show redirector <name> status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show redirector urlmethod

Description Shows the URL method setting of the redirector.

Syntax `show redirector <name> urlmethod`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show route

Description Shows the destination IP address, gateway address, and netmask of each route in the routing table.

Syntax `show route`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server

Description Shows the server configuration.

Syntax `show server`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Global Configuration

show server compression Commands

Use the show server compression commands to view the server compression settings.

show server compression

Description Shows the server compression settings.

Syntax `show server compression`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression 2k_padding

Description Shows whether 2k padding is enabled for compression.

Syntax `show server compression 2k_padding`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression browser

Description Shows the compression setting for all web browsers or a specific browser type.

Syntax

```
show server compression browser [ie4 | ie5 | ie51 | ie55 | ie6 | ie7 | ieother |
konqueror | ns4 | ns6 | opera | other | safari]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression cmt

Description Shows the CMT setting: 1, 2, or 3.

Syntax

```
show server compression cmt [1 | 2 | 3]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression cmt status

Description Shows the compress CMT status: disabled or enabled.

Syntax

```
show server compression cmt status
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression flushthreshold

Description Shows if flush threshold compression is enabled.

Syntax `show server compression flushthreshold`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression force

Description Shows if the compression algorithm is forced:

- 0 = none
- 1 = gzip
- 2 = deflate

Syntax `show server compression force`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression http10

Description Shows if HTTP 1.0 is being compressed.

Syntax `show server compression http10`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression javascript

Description Shows if application/x-javascript will be compressed.

Syntax `show server compression javascript`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression level

Description Shows the compression level.

Syntax `show server compression level`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression msoffice

Description Shows if MS Office documents will be compressed.

Syntax `show server compression msoffice`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression octetstream

Description Shows if application/octet-stream will be compressed.

Syntax `show server compression octetstream`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression optimization

Description Shows if compression optimization is enabled.

Syntax `show server compression optimization`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression policy

Description Shows if compression is enabled (set to zero).

Syntax `show server compression policy`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression shockwave

Description Shows if application/x-shockwave Flash will be compressed.

Syntax `show server compression shockwave`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server compression <text_>

Description Disables or enables compression for each type of text (CSS, HTML, and plain text are enabled by default).

This command does not take effect until after a `write` operation.

Syntax `show server compression <text_css | text_html | text_plain | text_xcomponent | text_xml> <disabled | enabled>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show server customiplogheader

Description Shows the custom header name that will be added to the client's request with the client's original IP address.

Syntax `show server customiplogheader`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server failover

The service-specific failover commands are listed in “Service Failover Commands” on page 479. These commands have been replaced by the commands for Unified Failover (refer to “show failover Commands” on page 405).

show server forwardclientcert

Description Shows the custom SSL client certificate HTTP header.

Syntax `show server forwardclientcert`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server maxconns

Description Shows the maximum number of simultaneous connections that the DX can support.

Syntax `show server maxconns`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server reversepath Commands

Use the show server reversepath commands to view the reverse path routing settings.

show server reversepath

Description Displays the current configuration of the Reversepath Routing feature.

Syntax `show server reversepath`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show server reversepath entries

Description Displays the current entries that are created in the system.

Syntax `show server reversepath entries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show server reversepath maxroutes

Description Displays the maximum number of routes that are allowed.

Syntax `show server reversepath maxroutes`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show server reversepath timeout

Description Displays the current timeout value.

Syntax `show server reversepath timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show server stats Commands

Use the show server stats commands to view server statistics.

show server stats

Description Displays all server statistics including I/O, HTTP, and SSL statistics for the server. Typing a number (n) here repeatedly displays all server statistics every n seconds.

Syntax `show server stats [n]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Global Configuration

show server stats auth

Description Displays the server authentication statistics, including the number of password changes and failed authentications.

Syntax `show server stats auth`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Global Configuration

show server stats history

Description Use the `show server stats history` command to display the history statistics for the server.

Syntax `show server stats history`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen

Description Shows the historical listen statistics for the server.

Syntax `show server stats history http listen`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen browser

Description This option shows the connections by the type of browser. The browsers monitored are shown in Table 10 on page 378.

Syntax `show server stats history http listen browser`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen method

Description This option shows the request method. The methods that are monitored are shown in Table 11 on page 379.

Syntax `show server stats history http listen method`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen req-err

Description This option shows the illegal requests. The illegal requests are shown in Table 12 on page 379.

Syntax `show server stats history http listen req-err`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen request

Description Number of active client requests.

Syntax `show server stats history http listen request`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http listen version

Description Shows the client browser version as shown in Table 13 on page 379.

Syntax `show server stats history http listen version`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target

Description Show the historical target statistics for the server.

Syntax `show server stats history http target`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target bytesin

Description Shows the target bytes from servers sorted by content type as shown in Table 14 on page 380.

Syntax `show server stats history http target bytesin`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target bytesout

Description Shows the target bytes sent to users sorted by content type as shown in Table 14 on page 380.

Syntax `show server stats history http target bytesout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target content

Description Shows the types of content handled sorted by content type as shown in Table 14 on page 380.

Syntax `show server stats history http target content`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target decompression

Description Shows the historical statistics for decompression.

Syntax `show server stats history http target decompression [performed | failure] [day | hour | month | year]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history http target responsecode

Description Shows the quantity of each type of response code handled.

Syntax `show server stats history http target responsecode`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history io

Description Shows all of the client-side I/O statistics for the cluster, including:

- Bytes In (Req from Clients)
- Bytes Out (Resp to Clients)
- Current Client Connections
- Total Client Connections
- Refused Client Connections

Syntax

```
show server stats history io
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history io listen

Description Shows all of the server I/O listen historical statistics, or the statistics for the specified time frame.

Syntax

```
show server stats history io listen [day | hour | minute | month | second |
year]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history io target

Description Shows the server-side I/O cluster statistics, or the statistics for the specified time frame. The statistics include:

- Bytes-in (requests from clients)
- Bytes-out (response to clients) current active server connections

Syntax

```
show server stats history io target [day | hour | month | year]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history ssl

Description Shows the SSL statistics for the cluster including the number of:

- New Sessions
- Reused Sessions
- Sessions with Strong Encryption
- Sessions with Export Encryption
- Sessions using Version SSLv2
- Sessions using Version SSLv3
- Sessions using Version TLSv1
- Sessions using Version Other.

Syntax `show server stats history ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

show server stats history ssl listen

Description Shows all of the server SSL listen historical statistics, or the statistics for the specified time frame.

Syntax `show server stats history ssl listen [day | hour | minute | month | second | year]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats history ssl target

Description Shows all of the server SSL target historical statistics, or the statistics for the specified time frame.

Syntax `show server stats history ssl target [day | hour | month | year]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats http

Description Displays all HTTP statistics for the server.

Syntax `show server stats http`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats io

Description Displays all I/O statistics for the server.

Syntax `show server stats io`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show server stats ssl

Description Displays all SSL statistics for the server.

Syntax `show server stats ssl`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X			X	X		

Mode(s) Global Configuration

show server status

Description Shows if the server is up or down.

Syntax `show server status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show slb Commands

Use the show slb commands to view the configuration and statistics for the Server Load Balancer (SLB). The SLB statistics include:

- Active: The number of active sessions.
- Total: The total number of sessions successfully terminated.
- Close: The number of sessions in closewait state (waiting to be closed).
- SYNWait: The number of sessions in synwait state (a client sent a SYN and is waiting for a SYN/ACK from the server, or a server sent a SYN/ACK and is waiting for an ACK from the client).

show slb

Description Displays all SLB configuration settings.

Syntax `show slb`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						X

Mode(s) Server Load Balancer

show slb advanced

Description Displays whether a reset is sent to the client and server when a connection is terminated. You can also view just the client or server setting.

Syntax `show slb advanced [reset <client | server>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb failover

The service-specific failover commands are listed in “Service Failover Commands” on page 479. These commands have been replaced by the commands for Unified Failover (refer to “show failover Commands” on page 405).

show slb group

Description Displays the SLB settings for one or all groups.

Syntax `show slb group [<name>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Server Load Balancer

show slb group advanced

Description Displays whether a reset is sent to the client and server when a connection is terminated for the group. You can also view just the client or server setting.

Syntax `show slb group <name> advanced [reset <client | server>]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group healthcheck

Displays the group health check intervals when target hosts are down, for TCP SYN, and for when target hosts are up, and the maximum number of retries before a target is assumed to be down. You can also view a specific setting.

Syntax `show slb group <name> healthcheck [interval <down | syn | up> | maxtries]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group healthcheck smtp

Description Shows whether SMTP health checking for a group is enabled.

Syntax `show slb group <name> healthcheck smtp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show slb group listen qos

Description Shows the ToS/DSCP settings for client traffic from the SLB group.

Syntax `show slb group <name> listen qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

show slb group minhosts

Description Displays the minimum number of target hosts used for load balancing by priority.

Syntax `show slb group <name> minhosts`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group nat

Description Displays whether full or half Network Address Translation (NAT) is enabled.

Syntax `show slb group <name> nat`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group nat port

Description Displays the start or end of the range pf ports that are subject to NAT.

Syntax `show slb group <name> nat port <end | start>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group policy

Description Displays the load balancing policy for the group.

Syntax `show slb group <name> policy`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group priority

Description Displays whether priority-based load balancing is enabled for the group.

Syntax `show slb group <name> priority`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group protocol

Description Displays the protocol used for the group (TCP or UDP).

Syntax `show slb group <name> priority`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group service

Description Displays the service type for the group.

Syntax `show slb group <name> service`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group session

Description Displays the current sessions for one or all groups.

Syntax `show slb group <name | all> session`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group session timeout

Description Displays all the global purge timeouts for group sessions, or just the specified timeout.

Syntax `show slb session timeout [ackwait | active | closewait]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group stats

Description Displays the statistics for one or all groups.

Syntax `show slb group <name | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group sticky

Description Shows the sticky timeout, the cluster, forwarder, or SLB group that leads this SLB group, and the clusters, forwarders, and SLB groups that follow this SLB group. You can also show just the timeout, leader, or followers.

When a "leader" is configured, a client IP is bound to (follows) the same target host as another cluster, forwarder, or SLB group. This allows client applications with multiple protocol flows (such as TCP and UDP) to be load balanced to the same target host. The sticky method must be clientip.

Syntax `show slb group <name> sticky [leader | followers | timeout]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Server Load Balancer

show slb group sticky entries

Description Shows the clients currently associated with each target host.

Syntax `show slb group <name> sticky entries`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Server Load Balancer

show slb group sticky failover status

Description Shows the status of stateful failover for a the specified SLB group, including whether stateful failover is enabled or disabled, the address of the primary standby DX, and the start and end times for the most recent full and delta synchronization on this SLB group.

Syntax `show slb group <name> sticky failover status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Unified Failover

show slb group target host <ip:port>

Description Shows the status, priority, maximum connections, and weight for the specified target host. You can also view a specific setting.

Syntax `show cluster <name> target host <ip:port> [maxconns | status | weight]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				X

Mode(s) Server Load Balancer

show slb group target host <ip:port | all> session

Description Displays the current sessions for one or all target hosts in one or all groups.

Syntax `show slb group <name | all> target host <ip:port | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group target host <ip:port | all> stats

Description Displays statistics for one or all target hosts in one or all groups.

Syntax `show slb group <name | all> target host <ip:port | all> stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb group target qos

Description Shows the ToS/DSCP settings for the traffic sent to the target hosts.

Syntax `show slb group <name> target qos`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Server Load Balancer

show slb healthcheck

Displays the group health check intervals when target hosts are down, for TCP SYN, and for when target hosts are up, and the maximum number of retries before a target is assumed to be down. You can also view a specific setting.

Syntax `set slb group <name> healthcheck [interval <down | syn | up> | maxtries]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb session

Description Displays the current sessions.

Syntax `show slb session`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb session timeout

Description Displays all the global purge timeouts for SLB sessions, or just the specified timeout.

Syntax `show slb session timeout [ackwait | active | closewait]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats

Description Displays the overall statistics for the DX and all of error, healthcheck, memory, sticky, FTP, and TFTP stats displayed with the other `show slb stats` commands. Statistics are cumulative, except for memory and current sessions.

Syntax `show slb stats`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats errors

Description Displays error statistics for the SLB service, such as target host unavailable and connection timeouts. Statistics are cumulative.

Syntax `show slb stats errors`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats healthcheck

Description Displays healthcheck statistics for the SLB service, such as total probes, responses and timeouts. Statistics are cumulative.

Syntax `show slb stats healthcheck`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats memory

Description Displays memory statistics for the SLB service, including the current usage for NAT, NAT ports, and session memory, as well as the number of times memory allocation failed.

Syntax `show slb stats memory`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats sticky

Description Displays client IP sticky statistics for the SLB service, including the number of insertions and deletions that have been made into the sticky table, and the number of paused or down target hosts. Statistics are cumulative.

Syntax `show slb stats sticky`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats ftp

Description Displays FTP statistics for the SLB service, including the number of times PORT, PASV, EPSV, and EPRT commands and PASV and EPSV responses are issued. Statistics are cumulative.

syntax `show slb stats ftp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb stats tftp

Description Displays TFTP statistics for the SLB service, including the number of read (RRQ) and write (WRQ) requests issued. Statistics are cumulative.

Syntax `show slb stats tftp`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb status

Description Displays the SLB switch status, as shown in Table 18.

Table 18: SLB Switch Status

Switch Status	Meaning
Disabled	SLB is off.
Enabled (active)	SLB is enabled for failover and is the active switch.
Enabled (stand-alone)	SLB is in stand-alone mode.
Enabled (passive)	SLB is enabled for failover and is the backup switch.

Syntax `show slb status`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show slb sticky timeout

Description Displays the sticky idle timeout.

Syntax `show slb sticky timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Server Load Balancer

show snat Commands

show snat

Description Shows the maximum number of connections and maximum idle time for Source Network Address Translation (SNAT). You can also view just one setting.

Syntax `show snat [maxconn | idletime]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat group

Description Lists one or all SNAT groups.

Syntax `show snat group [name]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat group member

Description Shows all the members in a group.

Syntax `show snat group <name> member <name | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat group member ip

Description Shows a SNAT group member's IP address.

Syntax `show snat group <name> member <name> ip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat group member netmask

Description Shows a SNAT group member's IP netmask.

Syntax `show snat group <name> member <name> netmask`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat group vip

Description Shows the Virtual IP address for the group.

Syntax `show snat group <name> vip`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show snat sessions

Description Shows the current SNAT sessions.

Syntax `show snat sessions`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show sync group Commands

Description Use the `show sync group` commands to show the configuration of a synchronization group for configuration synchronization.

Starting with software release 4.1.15, the `set sync group` command is disabled on the DX 3670.

show sync group

Description Shows all of the settings for one or all synchronization groups.

Syntax `show sync group [name]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show sync group description

Description Shows the description for a synchronization group.

Syntax `show sync group <name> description`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show sync group member

Description Shows the username and password for the named synchronization group member or all synchronization group members.

Syntax `show sync group <name> member <id | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show sync group override

Description Shows whether the group override file is enabled and the file name. You can also view just one setting.

Syntax `show sync group <name> override [filename | status]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show sync group timeout

Description Shows the timeout value for the group.

Syntax `show sync group <name> timeout`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

show system debug

Description Shows debugging information.

Syntax `show system debug`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show system info

Description Shows the DX hardware model and current software version.

Syntax

```
show system info
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show tcpdump

Description Shows the TCP dump information for the specified TCP dump file. If the file is encrypted, use the -s option. The user can then be prompted for an optional keyfile password. The `tcpdump` command must be executed first (see “tcpdump Commands” on page 469).

Syntax

```
show tcpdump <tcpdumpfile> [-s] [keyfile]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show timezone

Description Shows the time zone on the DX or a list of all time zones. To set the time zone, see “set timezone” on page 307.

Syntax

```
show timezone [list]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show ua

Description Shows the DX End User License Agreement.

Syntax `show ua`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show user

Description Shows the status and role of one or all users. Only users with an administrator role may display this information. For example:

```
dx% show user
User        Class       Status      SSH Keys    Roles
----        -----       ------      --------    -----
admin       local       Enabled     no          administrator
user1       local       Enabled     no          administrator
user2       local       Enabled     no          network_administrator
user3       local       Enabled     no          network_operator
user4       local       Enabled     no          security_administrator
user5       local       Enabled     no          security_operator
user6       local       Enabled     no          user
user7       local       Enabled     no          (none)
user8       local       Enabled     no          target_host_operator
```

Syntax `show user [username]`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

show user ssh authorized_keys

Description Shows the specified user's public SSH key in a newline delimited format.

Admin-level users can execute this command to view the public key for any other user, but non-admin users can only execute this command to view their own public key.

Syntax `show user [name] ssh authorized_keys`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show user ssh authorized_keys raw

Description Shows the specified user's public SSH key. Unlike the `show user ssh authorized_keys` command, this command does not insert newlines when showing the key.

Admin-level users can execute this command to view the public key for any other user, but non-admin users can only execute this command to view their own public key.

Syntax `show user [name] ssh authorized_keys raw`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

Mode(s) Global Configuration

show version

Description Shows the version of the firmware in the active partition of the DX.

Syntax `show version`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

show vlan Commands

Use the `show vlan` commands to show virtual LAN settings.

show vlan

Description Shows all VLAN parameters.

Syntax `show vlan`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show vlan default

Description Shows the default VLAN parameters.

Syntax `show vlan default`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show vlan ip

Description Shows the VLAN parameters for a specific IP address or all IP addresses.

Syntax `show vlan ip <ip | all>`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

show vlan range

Description Shows the VLAN parameters for a range of IP addresses or all IP addresses.

Syntax
```
show vlan <startip-endip | all>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X				

Mode(s) Global Configuration

sync group

Description Synchronizes the configuration settings across a group of DXs. You can synchronize all settings, or just the GSLB settings. Before entering this command, you must define the synchronization group and configure the SOAP server. When adding members to the synchronization group, the local DX must be added along with all remote DXs that need to receive the group configuration.

Starting with software release 4.1.15, the `sync group <name>` command is disabled on the DX 3670.

This command takes effect immediately.

Syntax
```
sync group <name> <all | gslb>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

Mode(s) Global Configuration

tcpdump Commands

The `tcpdump` command consists of information useful for troubleshooting.

You must configure the mechanism to deliver the dump and filename for storing the TCPDump if you are using TFTP or SCP before executing this command:

```
set admin tcpdump filename <filename> (only needed for TFTP)
set admin tcpdump transport (scp | smtp | tftp)
```

Prior to Release 2.3, the TCPDump collected by the DX was encoded in base64. Beginning with Release 2.3, the TCPDump collected is in a binary format. To view the TCPDump online:

```
show tcpdump
```

TCPDumps collected prior to Release 2.3 can be viewed offline by decoding it from the base64 format using a standard utility such as `uudecode`. Once decoded, it can then be viewed with a standard TCPDump utility with the `–r` option. TCPDumps collected with Release 2.3 or later can be viewed directly with a standard TCPDump utility.

Running a new TCPDump will overwrite the prior dump collected. To copy the TCPDump from the DX for analysis, use the `copy tcpdump` command. For additional information, see "copy tcpdump" on page 81.

tcpdump

Description Executes the `tcpdump` command and collects the dump information into a file.

Syntax

```
tcpdump
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

tcpdump -i [ether<N>]

Description Collects HTTP traffic passing between the DX and a target host on one or more interfacesusing the optional filtering criteria. The `-print` option displays the file on-screen rather than sending it to a file.

Syntax

```
tcpdump [-i etherN] [-print] [filter]
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

Mode(s) Global Configuration

traceroute

Description Shows the route of packets sent to a specific host name or IP address.

Syntax

```
traceroute <hostname | ip>
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X			X	X

Mode(s) Global Configuration

tsdump

Description

Use the `tsdump` command to send the technical service dump to a SCP or TFTP server or to the email address configuration.

Technical Service dumps consist of information useful for remote troubleshooting. You must configure the mechanism to deliver the dump and filename for storing the technical service dump if you are using TFTP before executing this command:

```
set admin tsdump filename <filename> (only needed for TFTP)
set admin tsdump transport (scp | smtp | tftp)
```

Syntax

```
tsdump
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X					

unconfigure

Description

Use the `unconfigure` command to restore a DX to the its original manufacturing configuration. Some of the actions it performs include:

- Restoring the default configuration; deleting the current one
- Deleting any new keys and certificates
- Deleting any new apprule files (e.g. not nitro.tune)
- Deleting any new configuration synchronization override files
- Deleting all health check scripts
- Deleting all but the default user
- Resetting the password of the default user
- Deleting the login banner
- Resetting the first boot flag; forcing acceptance of the user agreement
- Rebooting the DX

Syntax

```
unconfigure
```

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X						

wall

Description Use the `wall` command to send a message to all users who are currently logged in.

Syntax `wall`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

who

Description Use the `who` command to display a list of users who are currently logged in.

Syntax `who`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

whoami

Description Use the `whoami` command to display the login name of the current user.

Syntax `whoami`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X	X	X

write

Description Use the `write` command to save the configuration. Use `reload` to revert back to the previous configuration and discard any changes that you have made since the last `write` command.

Syntax `write`

Roles

Admin	Network Admin	Network Operator	Security Admin	Security Operator	User	Target Operator
X	X	X	X	X		X

Appendix A
Glossary

Table 19: Glossary

Term	Description
Certfile	Certification file for SSL traffic.
Cipher	Cryptographic algorithm for a server and client to authenticate each other, transmit certificates, and establish session keys.
Ciphersuite	A set of ciphers.
Cluster	A cluster is a set of web servers to be accelerated. It listens for incoming web traffic on a specific virtual IP address and port, distributes it over the target hosts (web servers) in the cluster and then accelerates the outgoing web traffic. Typically all the web servers in a particular cluster serve identical content; that is, each cluster usually represents a distinct website or property.
Convert302protocol	Converts the 302 responses from HTTP to HTTPS or from HTTPS to HTTP.
Customiplogheader	A special header to annotate the log; showing the session that is being logged in an easily identifiable way.
Custom Header	This is custom HTTP header that will be added with the client's origin IP to the client's request.
Default Route	Also known as the "Gateway," this is the IP address of the machine the Accelerator talks with in order to access the outside world.
Direct Server Return (DSR)	Reduces the outgoing traffic channeled through a load balancer by allowing web servers to send their HTTP responses directly back to the requesting client without passing back through the load balancer. Enable this option on the Accelerator if the target web servers are configured to use DSR.
DNS Domain	Also known as the Domain Suffix; this will be used to resolve unqualified host names.
DNS Nameserver	The IP address of the primary name server for the Accelerator. This is the machine the Accelerator queries to resolve host names into IP addresses.
Ethernet 0 (ether0)	This is the primary ethernet port of the Accelerator and the interface through which web traffic travels.
Ethernet 1 (ether1)	Also known as the "heartbeat" port, Ethernet 1 is used to communicate with a second Accelerator configured as a cold-standby fail-over unit.
Farm	A set of web clusters, typically with each cluster serving a different purpose.
Fail-over	This specifies whether or not the Accelerator should act as a cold-standby fail-over unit for another Accelerator on the network. NOTE: both the active and the stand-by DX units should have this option enabled, and both units should have the same Virtual IP settings
Forwarder	A forwarder is a mechanism for forwarding traffic on to a set of servers. It listens for incoming traffic on a specific virtual IP address and port and distributes it over the target hosts. Unlike a cluster, a forwarder blindly forwards incoming traffic on to its target hosts. These typically are not web servers, and the forwarder does not attempt to accelerate the outgoing traffic. This is for non-HTTP traffic; the forwarder simply passes the traffic through without examining it.
Hostname	The fully qualified DNS name for the Accelerator.
Keyfile	Key file for SSL traffic.
Keypass	Password for the SSL key.
Layer 7 Health Checking	Checks whether the target hosts are available by periodically sending an HTTP request to a specific URL on the target hosts.

Table 19: Glossary

Layer 7 Health Check Request Interval	The number of seconds separating each health check request sent to the the target hosts. The valid range of values is 1 - 60 seconds.
Layer 7 Health Check Request URL Path	The URL path that is requested on a target host with each health check. The URL path must begin with a slash '/'.
Layer 7 Health Check Retry Threshold	The number of times a health check must fail before the target host is considered unavailable. The valid range of values is 1 - 20.
Layer 7 Health Check Resume Threshold	The number of times a health check must succeed before the target host is considered available. The valid range of values is 1 - 20.
Layer 7 Health Check Status Code	The HTTP response status code expected from a target host in response to a health check. For typical use, the status code should be set to 200.
Layer 7 Health Check Page Size	The page size expected from a target host in response to a health check. This is the number of bytes in the body of the HTTP response, as it would be indicated in an HTTP Content-Length header. This is an optional setting; to disable this setting, use the value -1.
Layer 7 Health Check Expect String	A string expected to appear somewhere in the HTTP response given to a health check. The expect string is searched for in the non-header portion of the HTTP response. It is case-sensitive and must be enclosed in double-quotes if there is whitespace in the string. The maximum length of the string is 64 bytes. This setting only applies to health check responses with the following MIME types: text/html, text/css, text/plain and text/xml. This is an optional setting.
Listen Port	The port on which the Accelerator listens for incoming web traffic; it is typically set to 80.
Listen IP Address	See Virtual IP Address.
Listen IP Netmask	See Virtual IP Netmask.
Log Host	The IP address of the server to which the Accelerator will be sending logging data.
Logging	Turns logging on or off. Remember that logging always exacts a performance penalty.
Media	Media is the mode in which an ethernet interface (ether0 and ether1) operates.
MTU	Maximum Transmission Unit (MTU) is the largest number of bytes of “payload” data a frame can carry, not counting the frame's header and trailer. The MTU should be set to 1500 for Ethernet. DO NOT change this value unless your switch and network are configured to work with a different MTU.
Netmask	A mask to filter out addresses that should not access the device.
NTP	Network Time Protocol. Specifies whether or not the Accelerator should listen for your NTP server.
RADIUS	Remote Authentication Dial In User Service
Redirector	A redirector is mechanism for redirecting requests to a single web server. It listens for incoming web requests on a specific virtual IP address and port and redirects the client to that web server. Unlike a cluster, a redirector does not allow web traffic to pass through the Accelerator. Instead, for every web request a redirector receives, the redirector sends the client back a redirect URL and forces it to resend its HTTP request to that URL.
Redirector Host	The host portion of the redirect URL sent by the redirector. That is, this is the web server to which the client should be redirected. The redirector host may be specified as either a hostname or an IP address.
Redirector Port	The port portion of the redirect URL sent by the redirector.
Redirector Protocol	The protocol portion of the redirect URL sent by the redirector. Valid values are HTTP and HTTPS.

Table 19: Glossary

Redirector URL Method	The manner by which the redirector specifies the path portion of the redirect URL. If the request method is selected, then the redirector will construct the redirect URL using the same URL path as the original request. If the custom method is selected, then the redirector will construct the redirect URL using a custom URL path. You must specify a custom URL path if the custom method is selected, and the custom URL path must begin with a slash '/'. For instance, if the request method is selected and the redirector receives a request for a page at '/path/page.html', then the redirect URL will look something like 'http://my.redirect.host/path/page.html'. However, if the custom method is selected and the custom URL path is set to '/custom/script.cgi?a=b', then the redirect URL will look something like 'http://my.redirect.host/custom/script.cgi?a=b' for any request received by the redirector.
RMMP	Redundancy Multicast Messaging Protocol. This messaging protocol enables health checking between appliances.
Route (Default)	Also known as the "Gateway". This is the IP address of the machine the Accelerator talks with in order to access the outside world.
Server	Accelerator service.
SSL	Secure Sockets Layer (SSL) is a protocol that defines a way for two network devices to communicate securely. You can enable SSL on the listen side to communicate with clients securely. You can enable SSL on the target side to communicate with the target hosts securely
SSL Protocol Version	There are three versions of SSL protocol: SSL version 1 (SSLv1), SSL version 2 (SSLv2) and Transport Layer Security version 1 (TLSv1). There are four SSL protocol modes in which the Accelerator can operate: ■ sslv2: Use SSLv2 only ■ sslv3: Use SSLv3 only ■ sslv23: Use SSLv2, SSLv3 and TLSv1 ■ tslv1: Use TLSv1 only
SSL Ciphersuite	A collection of cryptographic algorithms used by two network devices to authenticate one another, transmit certificates and establish session keys. There are four categories of cipher suites used by the DX: ■ all: Allow all supported SSL cipher suites ■ common: Allow only the fastest cipher suites from both the strong and export groups ■ export: Allow only the low security cipher suites suitable for export ■ strong: Allow only the highest security cipher suites suitable for use in the U.S.A.
SSL Certfile	The certificate file used when establishing SSL communication.
SSL Keyfile	The key file used when establishing SSL communication.
SSL Keypass	The password for the SSL Keyfile.
Sticky	Ties a client to a server via the cookie or the client's IP address.
Sticky Load Balancing	A method of load balancing that binds a client to a server via a cookie or the client's IP address. It ensures that all subsequent requests made by a client are directed to the same server that handled the initial request.
Target Host:Port	This is the IP address and accompanying port of the web server that the Accelerator will accelerate. Depending upon the Accelerator model, you may be able to enter IP addresses and ports for up to eight Target Hosts.
Target Name	This is the fully-qualified host name which clients use to reach your website or the servers you are accelerating.

Table 19: Glossary

Accelerator Statistics	The following Accelerator statistics are available: ■ Uptime: The elapsed time since the Accelerator was turned on. ■ Sessions (active/total): The number of TCP sessions that the Accelerator has handled. ■ Requests (active/total): The number of HTTP requests the Accelerator has received. ■ Bytes (in/out): The total amount, in bytes, of data the Accelerator has received from target hosts, and the total amount of data that the Accelerator has sent out to clients.
Virtual IP Address	This is the IP address to which all incoming web traffic should be routed. It should be different from the IP address(es) you specified on the Network Settings page.
Virtual IP Netmask	The proper subnet mask for a device with the given Virtual IP Address.
WebUI Port	This is the port on which the administration web server (WebUI) listens. For example, if you set this to 8090, you can connect to the DX by typing something like http://junipername.yourdomain.com:8090
WebUI SSL	Turn SSL on or off for the administration web server (WebUI). The first time, this must be performed in the Command Line Interface (CLI), and you will be prompted to generate a certificate.

Appendix B
Cipher Suites

The Cipher Suites that are supported are shown in Table 20. This information can also be found in the "Setting up the DX for SSL Traffic" chapter of the *Installation and Administration Guide for DXOS*.

Table 20: SSL Ciphersuites

Cipher Suite	Description
Common SSL Ciphers ■ RC4-MD5 ■ RC4-SHA ■ EXP-RC4-MD5 ■ EXP-RC2-CBC-MD5 ■ EXP1024-RC4-MD5 ■ EXP1024-RC2-CBC-MD5	The fastest cipher suites from both the Strong and Export groups.
Strong SSL Ciphers ■ RC4-MD5 ■ RC4-SHA ■ AES256-SHA ■ AES128-SHA ■ IDEA-CBC-SHA ■ IDEA-CBC-MD5	The highest-security cipher suites that are suitable for use in USA.
Export SSL Ciphers ■ EXP-RC4-MD5 ■ EXP-RC2-CBC-MD5 ■ EXP1024-RC4-MD5 ■ EXP1024-RC2-CBC-MD5 ■ DES-CBC-MD5 ■ DES-CBC-SHA	Lower-security cipher suites that are suitable for export.

Table 20: SSL Ciphersuites

Cipher Suite	Description
All SSL Ciphers	Strong and Export.
■ RC4-MD5	
■ RC4-SHA	
■ DES-CBC-MD5	
■ DES-CBC-SHA	
■ DES-CBC3-MD5	
■ DES-CBC3-SHA	
■ AES256-SHA	
■ AES128-SHA	
■ IDEA-CBC-SHA	
■ IDEA-CBC-MD5	
■ EXP-RC4-MD5	
■ EXP-RC2-CBC-MD5	
■ EXP1024-RC4-MD5	
■ EXP1024-RC2-CBC-MD5	

Appendix C

Service Failover Commands

Table 21 lists the service-specific failover commands that have been replaced by the commands for Unified Failover. You should disable failover for ActiveN, the DX server, and SLB, and configure Unified Failover for all supported services (refer to “set failover Commands” on page 215).

Table 21: Service-Specific Failover Commands

Command	Description
ActiveN Commands	
clear activen failover bindaddr	Clears the failover bind address for ActiveN.
set activen failover [disabled | enabled]	Used to disable or enable the failover mechanism.
set activen failover bindaddr <ip>	Used to set the bind address for the failover mechanism (default is not configured).
set activen failover forcemaster <disabled | enabled>	Used to force a device to be the master if it’s node ID is lower than the current master (default is disabled).
set activen failover mcastaddr <ip>	Used to set the multicast address for the failover mechanism.
set activen failover nodeid <number | auto>	Used to set the nodeid of the ActiveN failover unit. Setting nodeid to “auto” will result in a nodeid being generated automatically (default is auto)
set activen failover port peer <port>	Used to set the port for failover communication (default is 9200).
set activen failover vmac [disabled | enabled]	Used to disable or enable the Virtual MAC (default is disabled). Available only on the Ethernet 0 interface.
set activen failover vmac id <id>	Used to assign the Virtual MAC Address (VMAC) to the specified ID.
show activen failover	Shows the ActiveN-only failover settings.
Server Commands	
set server failover <disabled | enabled>	Use the set server failover command to disable or enable the DX server failover. The first server established with failover is the active server; the second is the standby server. Disabling the server failover command will also disable the server failover vmac commnad, if it was enabled.
set server failover linkfail count	Failover link failure count. The default is 4.
set server failover linkfail pollinterval	Failover link failure poll interval in milliseconds. The default is 500.
set server failover vmac <disabled | enabled>	Disables or enables the failover with a Virtual MAC (vmac) option. Available only on the Ethernet 0 interface.
set server failover vmac id	Failover Virtual MAC (vmac) ID. The valid range is 1 to 254. The default is 0.
show server failover <blank>	Shows the failover server.
show server failover linkfail <blank>	Shows all link fail information.
show server failover linkfail count	Shows the number of failures that have occurred.

Table 21: Service-Specific Failover Commands

Command	Description
show server failover linkfail pollinterval	Shows the link failure polling interval in milliseconds.
show server failover vmac	Shows the Virtual MAC address.
show server failover vmac id	Shows the Virtual MAC Address assigned to the specified ID.
SLB Commands	
clear slb failover bindaddr	Clears the failover bind address.
set slb failover < disabled | enabled >	Disables or enables the failover mechanism.
set slb failover bindaddr < ip >	Sets the bind address for the failover mechanism.
set slb failover forcemaster < disabled | enabled >	Enabling the forcemaster allows a switch to snatch the active status from another switch of higher nodeid. Disables or enables the forcemaster. The default is disabled.
set slb failover mcastaddr < ip addr >	Sets the multicast address for the failover mechanism.
set slb failover nodeid < number | auto >	Sets the nodeid of the SLB failover unit. Setting nodeid to “auto” results in the nodeid being generated automatically. The default is auto.
set slb failover port peer < port >	Sets the port for failover communication. The default is 9200.
set slb failover vmac < disabled | enabled >	Enables or disables the use of Virtual MAC on the interface (disabled by default). Available only on the Ethernet 0 interface.
set slb failover vmac id < id >	Sets the Virtual Router ID of the failover unit. The parameter ID is a number between one and 254, both inclusive. The default is 1.
show slb failover	Displays the failover status.